



**16/LT
WP 238**

Nuomonė 01/2016 apie sprendimo dėl ES ir JAV „privatumo skydo“ tinkamumo projektą

Priimta 2016 m. balandžio 13 d.

Ši darbo grupė įsteigta pagal Direktyvos 95/46/EB 29 straipsnį. Tai nepriklausoma Europos patariamoji institucija duomenų apsaugos ir privatumo klausimais. Grupės uždaviniai išdėstyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriatas yra Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato C direktorate (Pagrindinės teisės ir Europos Sąjungos pilietybė), B-1049 Briuselis, Belgija, kab. Nr. MO-59 02/013.

Interneto svetainė: http://ec.europa.eu/justice/data-protection/index_en.htm

SANTRAUKA

2016 m. vasario 29 d. Europos Komisija paskelbė komunikatą, sprendimo dėl tinkamumo projektą ir pridėtus tekstus, kurie sudaro naują transatlantinio keitimosi asmens duomenimis komerciniais tikslais sistemą: ES ir JAV „privatumo skydą“ (toliau – „privatumo skydas“), kuriuo siekiama pakeisti ankstesnį JAV „saugų uostą“, kurį Europos Sąjungos Teisingumo Teismas (toliau – ESTT) paskelbė negaliojančiu 2015 m. spalio 6 d. *Schrems* byloje.

Remdamasi Direktyvos 95/46/EB 30 straipsnio 1 dalies c punktu, 29 straipsnio darbo grupė (toliau – DG29) įvertino šiuos dokumentus, kad galėtų pateikti savo nuomonę apie sprendimo dėl tinkamumo projektą. DG29 įvertino tiek komercinius aspektus, tiek galimus nukrypimus nuo „privatumo skydo“ principų nacionalinio saugumo, teisėsaugos ir viešųjų interesų tikslais.

DG29 atsižvelgė į galiojančią ES duomenų apsaugos teisinę sistemą, kaip nurodyta Direktyvoje 95/46/EB, bei pagrindines teises į privatų gyvenimą ir duomenų apsaugą, kaip nurodyta Europos žmogaus teisių konvencijos 8 straipsnyje ir Europos Sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniuose. Grupė taip pat svarstė teisę į veiksmingas teisių gynimo priemones ir teisingą bylos nagrinėjimą, kaip nurodyta Chartijos 47 straipsnyje bei kaip įprasta su įvairiomis pagrindinėmis teisėmis susijusioje praktikoje.

Be to, analizėje atspindi ESTT motyvai *Schrems* byloje, nustatant Komisijos veiksmų laisvę vertinant tinkamumą. Tinkamumo reikalavimų tikrinimas ir kontrolė turi būti griežtai vykdomi, atsižvelgiant į pagrindines teises į privatumą ir duomenų apsaugą ir žmonių, kuriems gali turėti įtakos perdavimas, skaičių.

„Privatumo skydas“ turi būti vertinamas esamame tarptautiniame kontekste, pvz., atsižvelgiant į didelio duomenų kiekio atsiradimą ir augančius saugumo poreikius. Nuo tada, kai 2000 metais buvo priimtas sprendimas dėl „saugaus uosto“, asmens duomenų rinkimo ir naudojimo apimtys ir mastai gerokai išaugo. Europos duomenų apsaugos institucijos pabrėžia jų ginamų principų svarbą.

Visų pirma, DG29 palankiai vertina „privatumo skydo“ patobulinimus, palyginti su „saugaus uosto“ sprendimu. Grupė pažymi, kad derybininkai nagrinėjo daugelį „saugaus uosto“ trūkumų, kuriuos ji pabrėžė savo 2014 m. balandžio 10 d. rašte Komisijos pirmininko pavaduotojai V. Reding.

Dėl to, kad „privatumo skydo“ principai ir suteikiamos garantijos numatytos tiek sprendime dėl tinkamumo, tiek jo prieduose, informaciją sudėtinga rasti arba kartais ji yra netinkama. Tai prisideda prie bendro naujos sistemos aiškumo trūkumo, o duomenų subjektų, organizacijų ir duomenų apsaugos institucijų prieiga yra sudėtingesnė. Be to, naudojama kalba yra neaiški. Todėl DG29 primygtinai siūlo Komisijai užtikrinti, kad tai būtų aišku ir suprantama abiejose Atlanto pusėse.

Kalbant apie taikytinus teisės aktus, DG29 pabrėžia, kad jeigu sprendimas dėl „privatumo skydo“ tinkamumo priimamas remiantis Direktyva 95/46/EB, jis turi būti suderinamas su ES

duomenų apsaugos teisės sistema tiek apimčių, tiek terminologijos atžvilgiu. DG29 mano, kad peržiūra turi būti atlikta nedelsiant pradėjus taikyti Bendrąjį duomenų reglamentą, siekiant užtikrinti, kad sprendime dėl tinkamumo ir jo prieduose būtų užtikrintas aukštesnis reglamente siūlomos duomenų apsaugos lygis.

Dėl „privatumo skydo“ komercinių aspektų

Pagrindinis DG29 tikslas yra užtikrinti, kad atitinkamas asmens duomenų apsaugos lygis būtų palaikomas, kai asmeniniai duomenys apdorojami, remiantis „privatumo skydo“ nuostatomis. Nors DG29 nesitiki, kad „privatumo skydas“ bus vien išsami ES teisės sistemos kopija, ji mano, kad jame turi būti pateikti pagrindiniai principai ir jis turi užtikrinti „iš esmės lygiavertį“ apsaugos lygį.

Nepaisant „privatumo skydo“ patobulinimų, DG29 mano, kad kai kurie pagrindiniai duomenų apsaugos principai neatspindi sprendimo dėl tinkamumo projekte ir jo prieduose, kaip numatyta Europos teisės aktuose, arba jie buvo netinkamai pakeisti alternatyviomis sąvokomis.

Pavyzdžiui, duomenų saugojimo principas nėra aiškiai paminėtas ir negali būti aiškiai suformuluotas remiantis esama duomenų vientisumo ir tikslo ribojimo principo formuluote. Be to, nėra formuluočių apie apsaugą nuo automatizuotų sprendimų, paremtų tik automatiniu duomenų tvarkymu. Tikslo ribojimo principo taikymas duomenų tvarkymui taip pat yra neaiškus. Siekiant, kad kelių svarbių sąvokų naudojimas būtų aiškesnis, DG29 rekomenduoja, kad ES ir JAV sutartų aiškus apibrėžtis ir kad jos būtų pateiktos terminų žodyne, kuris turėtų būti įtrauktas į „privatumo skydo“ dažnai užduodamų klausimų skyrių.

Kadangi „privatumo skydas“ taip pat bus naudojamas duomenų perdavimui už JAV ribų, DG29 primygtinai ragina, kad tolesnis perdavimas iš „privatumo skydo“ subjekto gavėjams trečiojoje šalyje turėtų būti to paties apsaugos lygio visais „skydo“ aspektais (įskaitant nacionalinį saugumą), o ES duomenų apsaugos principai nebūtų apeinami. Jeigu pagal „privatumo skydą“ numatomas tolesnis perdavimas į trečiąją šalį, visos „privatumo skydo“ organizacijos turėtų būti įsipareigojusios įvertinti duomenų importuotojui taikomus būtinus trečiosios šalies nacionalinių įstatymų reikalavimus prieš perdavimą. DG29 tvirtina, kad tolesnis ES asmens duomenų perdavimas yra nepakankamai reglamentuotas, ypač jų apimtys, tikslo ribojimo ir perdavimui atstovams taikomų garantijų atžvilgiu.

Galiausiai, nors DG29 pažymi, kad asmenims skirta papildomų išteklių naudojimuisi teisėmis užtikrinti, ji yra susirūpinusi, kad naujasis teisių gynimo mechanizmas praktikoje gali būti per sudėtingas, jį gali būti sudėtinga naudoti ES esantiems asmenims ir todėl jis gali būti neveiksmingas. Todėl reikalingas tolesnis įvairių teisių gynimo procedūrų paaiškinimas; jeigu pageidaujama, ES piliečiams vykdant įvairias procedūras, ES duomenų apsaugos institucijos gali būti laikomos atstovėmis ryšiams, kurioms suteikiama galimybė veikti jų vardu.

Nukrypimai nacionalinio saugumo tikslais

Valdžios institucijų prieigos prie duomenų atžvilgiu, tiek ES, tiek trečiosiose šalyse DG29 primena savo atliktą susijusių pagrindinių teisių analizę, pateiktą darbiniam dokumente dėl kišimosi į pagrindines teises į privatumą ir duomenų apsaugą pateisinimo, asmens duomenų perdavimo metu taikant stebėjimo priemones (Europos esminės garantijos) (WP237).

Didžiulis žingsnis į priekį, palyginti su „saugaus uosto“ sprendimu, yra tas, kad dabar sprendimo dėl tinkamumo projektas iš esmės yra susijęs su galima prieiga prie pagal „privatumo skydą“ tvarkomų duomenų nacionalinio saugumo ir teisėsaugos tikslais. DG29 pripažįsta šį svarbų žingsnį bei JAV administracijos užtikrintą didesnę skaidrumą įstatymų, reglamentuojančių žvalgybos duomenų rinkimą (VI priedas), atžvilgiu.

Tačiau DG29 pažymi, kad JAV nacionalinės žvalgybos direktoriaus biuro (NŽDB) pareiškimuose neatmetamas masinis ir nesirinktinai vykdomas masto iš ES kylančių asmeninių duomenų rinkimas. DG29 pabrėžia savo ilgalaikę poziciją, kad masinis ir nesirinktinai asmenų stebėjimas niekada negali būti laikomas proporcingu ir griežtai būtinu demokratinėje visuomenėje, kaip reikalaujama, atsižvelgiant į pagrindinių teisių apsaugą. Be to, ypač svarbi išsami visų stebėjimo programų priežiūra. DG29 pažymi, kad pastebima tendencija masiškai ir nesirinktinai rinkti vis daugiau duomenų, prisidengiant kova prieš terorizmą. Atsižvelgdama į nerimą dėl pagrindinių teisių į privatumą ir duomenų apsaugą, DG29 laukia būsimų ESTT sprendimų bylose dėl masinio ir nesirinktinai vykdomo duomenų rinkimo.

Teisių gynimo atžvilgiu DG29 pritaria ombudsmeno institucijos kūrimui kaip naujam teisių gynimo mechanizmui. Tai gali būti žymus ES piliečių teisių pagerinimas JAV žvalgybos veiklos atžvilgiu. Tačiau DG29 nuogaštauja, kad ši nauja institucija nėra pakankamai nepriklausoma ir jai nesuteikta atitinkamų įgaliojimų, būtinų siekiant efektyviai vykdyti savo pareigas, ir ji neužtikrina patenkinamo teisių gynimo iškilus nesutarimams.

Bendra peržiūra

Sprendimo dėl tinkamumo projekte minėtas bendros metinės peržiūros mechanizmas yra pagrindinis bendro „privatumo skydo“ patikimumo veiksnys, o DG29 ypač pritaria suteiktai galimybei peržiūrėti sprendimą dėl tinkamumo. Šiuo atžvilgiu DG29 supranta, kad DG29 nacionaliniai atstovai aktyviai dalyvaus peržiūros procese, tačiau prašo paaiškinti tikslią tvarką. Prieš atliekant pirmąją peržiūrą, būtina išsamiai aptarti sąlygas (įskaitant sudarytą ataskaitą, jos paskelbimą ir galimas pasekmes bei finansavimą).

Išvada

DG29 atkreipia dėmesį į didžiausius patobulinimus, kuriuos užtikrina „privatumo skydas“, palyginti su panaikintu sprendimu dėl „saugaus uosto“. Atsižvelgdama į išreikštas abejones ir prašomus paaiškinimus, DG29 ragina Komisiją išspręsti šiuos klausimus, nurodyti tinkamus sprendimus ir pateikti prašomus paaiškinimus, siekdama patobulinti sprendimo dėl

tinkamumo projektą ir užtikrinti, kad „privatumo skydo“ užtikrinama apsauga iš esmės būtų lygiavertė ES užtikrinamai apsaugai.

TURINYS

SANTRAUKA	2
DĖL „PRIVATUMO SKYDO“ KOMERCINIŲ ASPEKTŲ	3
NUKRYPTIMAI NACIONALINIO SAUGUMO TIKSLAIS	4
BENDRA PERŽIŪRA	4
IŠVADA	4
TURINYS	6
1. ĮVADAS	9
1.1. BENDROSIOS PASTABOS	9
1.1.1 DG29 ĮVERTINIMO APIMTYS	9
1.1.2 SPRENDIMO DĖL TINKAMUMO PROJEKTO KOMERCINĖS DALIES ĮVERTINIMAS	10
1.1.3 VALDŽIOS INSTITUCIJŲ IR JŲ TAIKOMŲ APSAUGOS PRIEMONIŲ PRIEIGOS NUKRYPTIMŲ ĮVERTINIMAS	11
1.2 SPRENDIMO DĖL TINKAMUMO PROJEKTAS	12
1.2.1 ES DUOMENŲ APSAUGOS SISTEMOS IR YPAČ DIREKTYVOS 95/46/EB PRINCIPŲ TAIKYMO SRITYS	12
1.2.2 „PRIVATUMO SKYDO“ DOKUMENTŲ AIŠKUMO TRŪKUMAS	12
1.2.3 BENDRA PERŽIŪRA IR SUSTABDYMAS	14
1.2.4 PERSVARSTOMA ES TEISINĖ SISTEMA	15
2. SPRENDIMO DĖL TINKAMUMO PROJEKTO KOMERCINĖS DALIES ĮVERTINIMAS	15
2.1. BENDROSIOS PASTABOS	15
2.1.1 PATOBULINIMAI	15
2.1.2 „PRIVATUMO SKYDO“ TAIKYMAS ORGANIZACIJOMS, KURIOS VEIKIA KAIP DUOMENŲ TVARKYTOJOS (ATSTOVĖS)	15
2.1.3 ĮSIPAREIGOJIMO LAIKYTIS PRINCIPŲ APRIBOJIMAI	16
2.1.4 DUOMENŲ SAUGOJIMO APRIBOJIMŲ PRINCIPŲ TRŪKUMAS	17
2.1.5 AUTOMATIZUOTŲ SPRENDIMŲ GARANTIJŲ TRŪKUMAS, DĖL KURIO KYLA TEISINĖS PASEKMĖS ARBA LABAI PAKENKIAMA ASMENIUI	17
2.1.6 ESAMŲ KOMERCINIŲ SANTYKIŲ TARPINIS LAIKOTARPIS	18
2.2. KITOS PASTABOS	18
2.2.1 SKAIDRUMAS	18
2.2.2 PASIRINKIMAS	19
2.2.3 TOLESNIS PERDAVIMAS	20
2.2.4 DUOMENŲ VIENTISUMAS IR TIKSLŲ RIBOJIMAS	23
2.2.5 DUOMENŲ SUBJEKTŲ PRIEIGOS, TAISYMO IR IŠTRYNIMO TEISĖ	25
2.2.6 TEISIŲ GYNIMAS, REIKALAVIMŲ UŽTIKRINIMAS IR ATSAKOMYBĖ (TEISIŲ GYNIMO MECHANIZMAI)	26
2.2.7 ŽMOGIŠKŲJŲ IŠTEKLIŲ DUOMENŲ TVARKYMAS	30
2.2.8 FARMACINIAI IR MEDICINOS PRODUKTAI	31
2.2.9 VIEŠAI PRIEINAMA INFORMACIJA	33
2.3 IŠVADOS	33
3. SPRENDIMO DĖL TINKAMUMO PROJEKTO NACIONALINIO SAUGUMO GARANTIJŲ ĮVERTINIMAS	33

3.1 JAV NACIONALINIO SAUGUMO ĮSTAIGOMS TAIKOMOS APSAUGOS PRIEMONĖS IR APRIBOJIMAI	33
3.2 A GARANTIJA: DUOMENŲ TVARKYMAS TURI ATITIKTI ĮSTATYMUS IR BŪTI PAREMTAS AIŠKIOMIS, TIKSLIOMIS IR PRIEINAMOMIS TAISYKLĖMIS	34
3.2.1 VYKDOMASIS ĮSAKAS NR. 12333 IR PREZIDENTO POLITINĖ DIREKTYVA NR. 28	35
3.2.2 UŽSIENIO ŽVALGYBOS STEBĖJIMO AKTAS	36
3.2.3 IŠVADA	37
3.3 B GARANTIJA: TURI BŪTI ĮRODYTAS BŪTINUMAS IR PROPORCINGUMAS, ATSIŽVELGIANT Į SIEKIAMUS TEISĖTUS TIKSLUS	37
3.3.1 PREZIDENTO POLITINĖ DIREKTYVA NR. 28	37
3.3.2 UŽSIENIO ŽVALGYBOS STEBĖJIMO AKTAS	38
3.3.3 IŠVADA	39
3.4 C GARANTIJA: TURĖTŲ BŪTI SUKURTAS NEPRIKLAUSOMAS PRIEŽIŪROS MECHANIZMAS	40
3.4.1 VIDINĖ PRIEŽIŪRA	40
3.4.2 IŠORINĖ PRIEŽIŪRA	41
3.4.3 IŠVADA	42
3.5 D GARANTIJA: ASMENIMS TURI BŪTI UŽTIKRINTOS VEIKSMINGOS TEISIŲ GYNIMO PRIEMONĖS	42
3.5.1 TEISMINĖS GYNYBOS PRIEMONĖS	42
3.5.1.1 IEŠKINIO TEISĖS REIKALAVIMAS	42
3.5.1.2 PREZIDENTO POLITINĖ DIREKTYVA NR. 28	43
3.5.1.3 UŽSIENIO ŽVALGYBOS STEBĖJIMO AKTAS	43
3.5.2 ADMINISTRACINĖS TEISIŲ GYNYBOS PRIEMONĖS	44
3.5.2.1 GENERALINIAI INSPEKTORIAI	44
3.5.2.2 INFORMACIJOS LAISVĖS AKTAS	44
3.5.3 „PRIVATUMO SKYDO“ OMBUDSMENAS	44
3.5.3.1 OMBUDSMENO SKYRIMAS	44
3.5.3.2 NAUJO OMBUDSMENO MECHANIZMO ĮVERTINIMAS	45
3.5.3.3 AR GALI PAKAKTI VIEN OMBUDSMENO PASKYRIMO ?	46
3.5.3.4 OMBUDSMENO MECHANIZMO TAIKymo APIMTIS	47
3.5.3.5 TEISĖ REIKŠTI IEŠKINĮ IR PRAŠYMŲ TEIKIMO TVARKA	48
3.5.3.6 NEPRIKLAUSOMYBĖ	48
3.5.3.7 TYRIMO ĮGALIOJIMAI	49
3.5.3.8 ĮGALIOJIMAI IMTIS TAISOMŲJŲ VEIKSMŲ	50
3.5.4 IŠVADOS	50
3.6 BAIGIAMOSIOS PASTABOS DĖL JAV NACIONALINIO SAUGUMO ĮSTAIGOMS TAIKOMŲ APSAUGOS PRIEMONIŲ IR APRIBOJIMŲ	51
4. „PRIVATUMO SKYDO“ TEISĖSAUGOS GARANTIJŲ ĮVERTINIMAS	51
4.1 ĮVADAS	51
4.2 ESMINIŲ EUROPOS GARANTIJŲ TAIKYMAS TEISĖSAUGOS INSTITUCIJŲ PRIEIGAI PRIE KORPORACIJŲ TURIMŲ DUOMENŲ	52
4.2.1. TEISĖSAUGOS INSTITUCIJŲ PRIEIGA PRIE ASMENS DUOMENŲ TURI ATITIKTI ĮSTATYMUS IR TURI BŪTI PAREMTA AIŠKIOMIS, TIKSLIOMIS IR PRIEINAMOMIS TAISYKLĖMIS	52
4.2.2 TURI BŪTI ĮRODYTAS BŪTINUMAS IR PROPORCINGUMAS, ATSIŽVELGIANT Į SIEKIAMUS TEISĖTUS TIKSLUS	52
4.2.3 TURĖTŲ BŪTI SUKURTAS NEPRIKLAUSOMAS PRIEŽIŪROS MECHANIZMAS	54
4.2.4 ASMENIMS TURI BŪTI UŽTIKRINTOS VEIKSMINGOS TEISIŲ GYNIMO PRIEMONĖS	54
4.3 BAIGIAMOSIOS PASTABOS	55

5. IŠVADOS IR REKOMENDACIJOS	56
5.1 TRYS NERIMĄ KELIANTYS KLAUSIMAI	56
5.2 REKOMENDUOJAMI PAAIŠKINIMAI	56

1. ĮVADAS

Remdamasi Europos Sąjungos Teisingumo Teismo (toliau – ESTT) 2015 m. spalio 6 d. *Schrems* byloje priimtu sprendimu¹, 29 straipsnio Darbo grupė (toliau – DG29, Darbo grupė) Europos Sąjungos (toliau – ES) valstybes nares ir kitas Europos institucijas paragino pradėti diskusijas su Jungtinių Valstijų (toliau – JAV) valdžios įstaigomis, siekiant priimti politinius, teisinius ir techninius sprendimus, sudarančius sąlygas duomenų perdavimui į JAV teritoriją, kuriais būtų paisoma pagrindinių teisių.

2016 m. vasario 2 d., po daugiau nei dvejų metų trukmės derybų, Europos Komisija ir JAV prekybos departamentas (PD) sudarė politinį susitarimą dėl *Naujos transatlantinio keitimosi asmens duomenimis komerciniais tikslais sistemos: ES ir JAV „privatumo skydo“* (toliau – „privatumo skydas“), kuriuo siekiama pakeisti ankstesnįjį JAV „saugų uostą“.

2016 m. vasario 29 d. Komisija paskelbė komunikatą², sprendimo dėl tinkamumo projektą ir pridėtus tekstus, kurie sudarys „privatumo skydą“. Remdamasi Direktyvos 95/46/EB (toliau – Direktyva) 30 straipsnio 1 dalies c punktu, DG29 įvertino šiuos dokumentus, siekdama pateikti savo nuomonę apie Komisijos parengtą sprendimo dėl tinkamumo projektą, įskaitant pagrindžiamuosius „privatumo skydo“ dokumentus. Įvertinimo metu DG29 atskyrė „privatumo skydo“ komercinės dalies įvertinimą ir naudojamų apsaugos priemonių analizę, atsižvelgdama į nukrypimus nuo „privatumo skydo“ principų nacionalinio saugumo, teisėsaugos ir viešųjų interesų tikslais.

Remdamasi nutarimu *Schrems* byloje, DG29 surengė kelis susitikimus su delegacijomis iš JAV administracijos, pilietinės visuomenės organizacijų atstovais iš ES ir JAV bei mokslininkais, siekdama įvertinti nutarimo *Schrems* byloje pasekmes. Vertinant „privatumo skydą“, buvo surengti kiti susitikimai su Europos Komisijos ir JAV administracijos atstovais. Šių susitikimų metu buvo pateikti paaiškinimai, į kuriuos taip pat buvo atsižvelgta šioje nuomonėje. DG29 pabrėžia, kad šiame etape paaiškinimai buvo neoficialūs ir jie nėra sprendimo dėl tinkamumo sudedamoji dalis, kadangi jie kol kas neįforminti raštiškai.

Nepaisant to, DG29 ypač palankiai vertina šių susitikimų metu priimtą PD įsipareigojimą bendradarbiauti su ES valstybių narių duomenų apsaugos institucijomis „privatumo skydo“ nuostatų taikymo klausimais ir teikti nurodymus bei teisinius paaiškinimus apie „privatumo skydo“ taikymą, kurie turi būti skelbiami jų internetinėse svetainėse.

1.1. Bendrosios pastabos

1.1.1 DG29 įvertinimo apimtys

Visų pirma, DG29 atsižvelgė į Europos Sąjungos valstybėse narėse taikomą duomenų apsaugos sistemą, įskaitant Europos žmogaus teisių konvencijos (toliau – EŽTK) 8 straipsnį, užtikrinantį teisę į privatą ir šeimyninį gyvenimą bei Europos Sąjungos pagrindinių teisių

¹ 2015 m. spalio 6 d. sprendimas byloje *Maximilian Schrems/Data Protection Commissioner*, C-362/14 (toliau – *Schrems*).

² COM(2016) 117 final, 2016 m. vasario 29 d.

chartijos (toliau – Chartija) 7, 8 ir 47 straipsnius, atitinkamai apsaugančius teisę į privatų ir šeimyninį gyvenimą, teisę į asmens duomenų apsaugą ir teisę į veiksmingą teisių gynybą ir teisingą bylos nagrinėjimą. Grupė taip pat atsižvelgė į atitinkamą teisminę praktiką ir direktyvos reikalavimus.

Reikalavimas trečiajai šaliai užtikrinti atitinkamą duomenų apsaugos lygį ESTT buvo patikslintas Schrems byloje. Teismas, be kita ko, paaiškino, kad direktyvos nuostatos turi būti aiškinamos „atsižvelgiant į pagrindines Chartijos užtikrintas teises“³, o ypač 7 ir 8 straipsnius. Jis taip pat nurodė, kad formuluotė „tinkamas apsaugos lygis“ turi būti suprantama kaip „reikalavimas, kad trečioji šalis, remdamasi vietos įstatymais ar tarptautiniais įsipareigojimais, faktiškai užtikrintų atitinkamą pagrindinių teisių ir laisvių apsaugos lygį, kuris iš esmės atitinka pagal direktyvos ir Chartijos nuostatas Europos Sąjungoje užtikrintą lygį“⁴. Ankstesnio „saugaus uosto“ sprendimo atveju toks pakankamai išsamus įvertinimas niekada nebuvo atliktas. Todėl DG29 įvertino sprendimo dėl tinkamumo projektą, atsižvelgdama į reikalavimą pateikti pagrindinių teisių ir laisvių apsaugos lygio, kuris iš esmės atitinka ES garantuotą lygį, analizę. DG29 pabrėžia, kad šioje nuomonėje pateikiamos jos pagrindinės abejonės, tačiau nuo sprendimo dėl tinkamumo projekto paskelbimo praėjus tam tikram laikotarpiui, gali būti nustatyta kitų problemų.

DG29 pripažįsta, kad ESTT, apibrėždamas žodį „tinkamas“, pateiktą direktyvos 25 straipsnio 6 dalyje, kaip „iš esmės tinkamas“, išsamiau paaiškino tinkamumą Schrems byloje. Teismas taip pat pabrėžė, kad formuluotė „tinkamas apsaugos lygis“ turi būti suprantama kaip „reikalavimas, kad trečioji šalis, remdamasi vietos įstatymais ar tarptautiniais įsipareigojimais, faktiškai užtikrintų atitinkamą pagrindinių teisių ir laisvių apsaugos lygį, kuris iš esmės atitinka pagal direktyvos ir Chartijos nuostatas Europos Sąjungoje užtikrintą lygį“, tačiau trečiosios šalies nereikalaujama užtikrinti ES teisinės sistemos užtikrinamo apsaugos lygio.

1.1.2 Sprendimo dėl tinkamumo projekto komercinės dalies įvertinimas

DG29 jau paaiškino, kaip ji taikė pagrindinius ES duomenų apsaugos principus asmens duomenų perdavimui trečiosioms šalims savo 12 darbiname dokumente „Asmens duomenų perdavimas trečiosioms šalims: ES duomenų apsaugos direktyvos 25 ir 26 straipsnio taikymas“⁵. DG29 bandė rasti tinkamas apsaugos priemones, kurios užtikrintų tam tikrą apsaugos lygį, atitinkantį direktyvoje nurodytus principus, ypač dėl tikslo ribojimo, duomenų kokybės ir proporcingumo, skaidrumo, saugumo, prieigos teisių, taisymo ir užginčijimo, duomenų saugojimo ir tolesnio perdavimo apribojimų. Panašus metodas buvo taikomas DG29 įvertinant pradinį sprendimą dėl „saugaus uosto“ tinkamumo⁶ ir teikiant nuomonę bei Darbo

³ Schrems, 38 sk.

⁴ Schrems, 73 sk.

⁵ Priimta DG29 1998 m. liepos 24 d., žr. 6 p.

⁶ Žr. WP62, WP32, WP27, WP23, WP21, WP19, WP15 ir WP7.

grupės rekomendacijas rašte buvusiai Komisijos pirmininko pavaduotojai ir ES teisingumo komisarei Viviane Reding, paskelbtame 2014 m. balandžio 10 d.⁷

1.1.3 Valdžios institucijų ir jų taikomų apsaugos priemonių prieigos nukrypimų įvertinimas

Valdžios institucijų prieigos prie asmens duomenų, kuriems galioja „privatumo skydas“, nukrypimų įvertinimas yra sudėtingas, ypač atsižvelgiant į didesnę duomenų apsaugos institucijų ir visuomenės informuotumą apie JAV stebėjimo programas, remiantis atskleista informacija. Darbo grupė pripažįsta JAV administracijos pastangas didinti stebėjimo programų skaidrumą ir ketinimus į „privatumo skydą“ įtraukti papildomas apsaugos priemones, ir šioms pastangoms pritaria. Tuo pat metu DG29 pabrėžia, kad bet kokia pagrindinėms teisėms į privatų gyvenimą ir duomenų apsaugą ir duomenų apsaugai kylanti grėsmė demokratinėje visuomenėje turi būti pateisinama. ESTT kritikavo faktą, kad „saugaus uosto“ sprendime nebuvo pateikta informacijos apie Jungtinėse Amerikos Valstijose priimtų taisyklių, skirtų riboti bet kokią grėsmę, egzistavimą. Be to, nenurodoma, kad egzistuoja veiksminga teisinė apsauga nuo tokio tipo grėsmės⁸.

Todėl DG29 išanalizavo esamą JAV teisinę sistemą ir JAV žvalgybos agentūrų praktiką, kaip aprašyta prieduose prie sprendimo projekto bei sąlygose, pagal kurias leidžiamas pagrindinių teisių į privatų gyvenimą ir duomenų apsaugą, reglamentuotą Europos teisinėje sistemoje, pažeidimas.

Siekiant įvertinti, ar demokratinėje visuomenėje būtų pateisinamas bet koks teisių pažeidimas, įvertinimas buvo atliekamas, atsižvelgiant į Europos teismų praktiką pagrindinių teisių srityje, kurioje nustatytos keturios esminės žvalgybos veiklos garantijos⁹:

- A. Duomenų tvarkymas turi būti vykdomas remiantis įstatymais ir vadovaujantis aiškiomis, tikslėmis ir prieinamomis taisyklėmis: tai reiškia, kad kiekvienas pagrįstai informuotas asmuo turėtų galėti numatyti, kas gali atsitikti su jo duomenimis, kai jie perduodami;
- B. Reikalingumas ir proporcingumas teisėtų tikslų atžvilgiu turi būti įrodytas: turi būti nustatyta pusiausvyra tarp tikslo, kuriuo renkami duomenys ar prie kurių gaunama prieiga, ir asmens teisių;
- C. Turėtų egzistuoti nepriklausomas veiksmingas ir nešališkas priežiūros mechanizmas: tai gali būti teisėjas arba kita nepriklausoma institucija, kuri turėtų turėti pakankamus įgaliojimus reikalingiems patikrinimams atlikti;
- D. Asmeniui turi būti suteikta galimybė naudotis veiksmingomis teisių gynimo priemonėmis: visi turi turėti teisę ginti savo teises nepriklausomoje institucijoje.

⁷ http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

⁸ Schrems, 87, 88 sk.

⁹ Esminės Europos garantijos pagrįstos ESTT ir EŽTT teismų praktika ir išsamiau apibūdintos DG29 darbo dokumente WP237, paskelbtame 2016 m. balandžio 13 d.

1.2 Sprendimo dėl tinkamumo projektas

Visų pirma, DG29 palankiai vertina tai, kad nauja tinkamumo įvertinimo procedūra gali būti įdiegta praėjus mažiau nei šešiams mėnesiams nuo tada, kai ESTT „saugaus uosto“ sprendimą paskelbė negaliojančiu. Atsižvelgiant į kasdienių duomenų perdavimų tarp ES ir JAV skaičių, kuris, kaip DG29 pripažįsta, yra gyvybiškai svarbi ekonomikos dalis abiejose Atlanto pusėse, teisinis aiškumas reikalingas kuo greičiau.

Tačiau DG29 apgailestauja, kad Komisijos paskelbtame sprendimo dėl tinkamumo projekte nepateikiamas išsamus JAV vietos įstatymų ir tarptautinių įsipareigojimų įvertinimas tinkamumo ataskaitos forma, kuris anksčiau įprastai buvo atliekamas vykdant panašias procedūras ir remiantis direktyvos 25 straipsniu. Todėl DG29 neatliks išsamios teisinių aplinkybių, kurioms esant bus naudojamas „privatumo skydas“, analizės. Pavyzdžiui, grupė pažymi, kad esamame sprendimo dėl tinkamumo projekte nepateikiamos išvados dėl privatumo ir duomenų apsaugos įstatymų, kurie galioja JAV (tiek federaliniu, tiek valstybiniu lygmeniu), įskaitant sektorių teisės aktus, bei dėl teisės aktų, pagal kuriuos leidžiama vieša prieiga su stebėjimu nesusijusiomis formomis. Be to, sąryšis tarp duomenų perdavimo pagal „privatumo skydą“ ir kitas tinkamumo nuostatas, pvz., ES ir JAV Keleivių duomenų įrašų (KDI) sutartį ir Terorizmo finansavimo sekimo programos (TFSP) sutartį, neapibrėžtas.

1.2.1 ES duomenų apsaugos sistemos ir ypač Direktyvos 95/46/EB principų taikymo sritys

DG29 primena, kad pagal ES duomenų apsaugos teisinę sistemą ir ypač pagal direktyvą (4 straipsnio 1 dalį), valstybių narių įstatymai galioja ne tik jų teritorijoje įsikūrusių duomenų valdytojų atliekamoms duomenų tvarkymo procedūroms, bet ir kai duomenų valdytojai (nors ir nėra įsteigti ES teritorijoje) naudojami įranga, esančia ES teritorijoje, ypač asmens duomenų rinkimo tikslais. Dėl to ES valstybės narės įstatymai galioja bet kokioms duomenų tvarkymo procedūroms, kurios vykdomos iki perdavimo JAV, atsižvelgiant į ES įsikūrusios organizacijos veiklą arba naudojantis įranga, kuri įrengta ES, tačiau naudojama ne ES įsikūrusios organizacijos. DG29 reikalauja, kad tai būtų aiškiai nurodyta sprendimo dėl tinkamumo projekte.

Turėtų būti aišku, kad „privatumo skydo“ principai bus taikomi nuo duomenų perdavimo momento. Be to, DG29 primena, kad ES įsteigtiems duomenų valdytojams, kurie perduoda duomenis duomenų tvarkytojui JAV, galioja ES duomenų apsaugos įstatymai.

1.2.2 „Privatumo skydo“ dokumentų aiškumo trūkumas

Dėl to, kad „privatumo skydo“ principai ir suteikiamos garantijos numatytos tiek sprendime dėl tinkamumo, tiek jo prieduose, informaciją sudėtinga rasti arba kartais ji yra netinkama. Tai prisideda prie bendro naujos sistemos aiškumo trūkumo, o duomenų subjektų, organizacijų ir duomenų apsaugos institucijų prieiga prie jų yra sudėtingesnė. Be to, naudojama kalba yra neaiški. Todėl DG29 primygtinai siūlo Komisijai užtikrinti, kad tai būtų aišku ir suprantama abiejose Atlanto pusėse.

DG29 rekomenduoja pridėti atskirą priedą, kuriame turi būti apibrėžti pagrindiniai terminai, naudojami „privatumo skydo“ dokumentuose. Bendras ir nedviprasmiškas sprendime dėl „privatumo skydo“ tinkamumo apibrėžtas jame numatytų įsipareigojimų supratimas yra būtinas siekiant, kad jis efektyviai funkcionuotų abiejose Atlanto pusėse, o DG29 nuogąstauja, kad dėl daugybės kryžminių nuorodų ir nesuderintų formuluočių bei dėl to, kad sistemos dokumentai yra sudėtingi, iškils su „privatumo skydo“ įgyvendinimo suderinamumu, suprantamumu ir aiškumu susijusių sunkumų.

Dar daugiau, „privatumo skydo“ dokumentuose naudojama terminologija, kuri nesuderinama su ES duomenų apsaugos srityje įprastai naudojamu žodynu. Tai nebūtinai yra problema, jeigu aišku, kokia būtų atitinkama terminologija pagal ES įstatymus (ir pagal JAV įstatymus). Tačiau DG29 apgailestauja, kad šiuo atveju taip nėra, įskaitant sprendimo dėl tinkamumo projektą. Pavyzdžiui, žodis „prieiga“ naudojamas sprendimo dėl tinkamumo projekto 3 skyriuje asmens duomenų rinkimo kontekste, o ne kaip leidimas kam nors peržiūrėti surinktus duomenis. Bendrovėms suteikta prieiga prie duomenų ir asmenų prieigos teisė yra dvi skirtingos sąvokos, kurių nereikėtų painioti.

DG29 pabrėžia, kad terminologija turėtų būti nuosekliai naudojama visuose dokumentuose, įskaitant sprendimo dėl tinkamumo projektą. Šiuo atveju taip nėra, pavyzdžiui, sąvokų „duomenų tvarkymas“ ir „asmens duomenys“ atveju. Jos abi yra apibrėžtos II priede, tačiau nenuosekliai naudojamos dokumentuose, o dėl to atsiranda apsaugos spragų.^{10,11}

DG29 palankiai vertina, kad kai kurių naudojamų terminų apibrėžtys buvo įtrauktos į dokumentus, sudarančius „privatumo skydą“. Tačiau tai negalioja įvairiems kitiems esminiams terminams, įskaitant „atstovas“ arba „tvarkytojas“, „raktu užkoduoti duomenys“, „nuasmeninti duomenys“ ir „ES asmuo“, kurie, DG29 nuomone, garantuoja aiškią apibrėžtį, dėl kurios sutinka tiek JAV, tiek ES, siekiant, kad vėliau išvengtų painiavos tiek „privatumo skydą“ naudojantys duomenų valdytojai, tiek tvarkytojai, priežiūros institucijos bei plačioji visuomenė. Lengvas sprendimas būtų prie „privatumo skydo“ dažnai užduodamų klausimų pridėti terminų žodyną.

¹⁰ Kai kuriuose straipsniuose tiesiog išvardijamos kelios duomenų tvarkymo operacijų rūšys, tačiau nenaudojamas terminas „duomenų tvarkymas“. Dėl to atsiranda apsaugos spragų. Pavyzdžiui, remiantis II priedo III.6.f skirsnyje pateikta formuluote, „privatumo skydo“ principai galioti, tik jeigu organizacija „saugo, naudoja arba atskleidžia“ gautus duomenis (t.y. ne kitais tikslais, kuriuos apima terminas „duomenų tvarkymas“, pavyzdžiui, rinkimo, įrašymo, pakeitimo, gavimo, konsultacijų ar ištrynimo). Duomenų apsauga taikoma tik asmeninės informacijos „kūrimui, palaikymui, naudojimui ar sklaidai“ (II priedo II.4 skirsnis). Asmens duomenų apibrėžtis taip pat apsiriboja „gautais“ ir „įrašytais“ duomenimis. Dar vienas pavyzdys yra Pranešimo principas (II priedo II.1.a.iv skirsnis), kuriuo remiantis sertifikuota organizacija turi informuoti asmenis apie tikslus, kuriais ji „renka ir naudoja“ duomenis apie juos. II priedo III.9.a.11 skirsnyje nurodyti tik duomenys, kurie „perduodami“ arba prie kurių buvo gauta „prieiga“. Netgi jeigu pasirodo, kad daugeliu tokių atvejų neketinama apriboti Principų apimtis ar sukurti apsaugos spragas, dėl nenuoseklios terminologijos padidėja tokių spragų rizika. Kadangi terminas „duomenų tvarkymas“ apibrėžtas Principuose, būtina jį naudoti nuosekliai, siekiant išvengti šiuo metu egzistuojančių spragų. Priešingu atveju liktų per daug vietos nenumatytam aiškinimui, dėl ko galimas netinkamas sprendimo formulotės aiškinimas.

¹¹ II priedo I.8.a skirsnyje pateikta „asmens duomenų“ apibrėžtis reiškia „duomenis apie nustatytą ar nustatytiną asmenį“. Tačiau remiantis papildomu principu, nurodoma, kad žmoniškųjų išteklių duomenų atžvilgiu Principai taikomi, tik kai „perduodami arba prieinami nustatyti įrašai“. DG29 mano, kad tokiu būdu sukuriamą galimybę tvarkyti asmens duomenis ne vadovaujantis duomenų apsaugos principais pagal ES įstatymus ir ne pagal bendrą asmens duomenų apibrėžtį pagal „privatumo skydą“.

DG29 taip pat nurodo teisėtus pagrindus tvarkyti slaptus duomenis pagal 1 papildomą principą (II priedo III.1 skirsnis), kai organizacija neturi gauti aiškaus sutikimo („*opt-in*“). Šis 1 papildomas principas gali būti suprantamas kaip išsamus teisinių pagrindų rinkti duomenis ES aprašymas, kadangi šis sąrašas yra panašus į Direktyvos 8 straipsnį. DG29 primena, kad slaptų duomenų apdorojimas pagal ES įstatymus (įskaitant jų rinkimą ir perdavimą) pagal Direktyvos 8 straipsnį turi būti vykdomas teisėtais pagrindais. „Privatumo skydas“ negali būti aiškinamas kaip alternatyvus tokio duomenų tvarkymo pagrindas. Pavyzdžiui, DG29 nuomone, JAV organizacija negali rinkti duomenų pagal ES įstatymus remdamasi JAV darbo teisės nuostatomis (žr. II priedo III.1.a.v skirsnį). Todėl DG29 pabrėžia, kad bet koks 1 papildomo principo aiškinimas gali privesti prie jo taikymo slaptiems duomenims, kurie jau buvo perduoti, juos surinkus ES teisėtais pagrindais, išvardytais Direktyvos 8 straipsnyje.

DG29 galiausiai pažymi, kad trūksta aiškumo klausimu, kas gali būti laikomas ES asmeniu ir tokiu būdu galima pasinaudoti „privatumo skydo“ suteikiama apsauga: visi ES piliečiai ar visi ES gyvenantys asmenys. Tai yra ypač svarbu teisės į teisių gynybą atžvilgiu, įskaitant prieigą prie ombudsmeno institucijos. Be to, sprendime dėl tinkamumo turi būti išspręstas klausimas, kiek „privatumo skydas“ galios EEE šalių ir Šveicarijos piliečiams / gyventojams, kuriems anksčiau galiojo „saugaus uosto“ sistema.

1.2.3 Bendra peržiūra ir sustabdymas

DG29 palankiai vertina tai, kad Europos Komisija ir JAV administracija susitarė reguliariai peržiūrėti praktinį „privatumo skydo“ naudojimą. Bendra peržiūra yra gerai žinoma ES duomenų apsaugos bendruomenės praktika daugelį metų, ypač sutarčių dėl keitimosi KDĮ duomenimis su trečiosiomis šalimis ir TFSP sutarties atžvilgiu. Be to, DG29 palankiai vertina tai, kad šiose bendrose peržiūrose gali dalyvauti neapibrėžtas duomenų apsaugos institucijų atstovų skaičius.

Atsižvelgdama į grupės patirtį bendrų peržiūrų srityje pastaraisiais metais, DG29 norėtų pabrėžti, kad ji tikisi, jog bendra „privatumo skydo“ apžvalga bus platesnė nei bendros KDĮ ir TFSP apžvalgos. Iš esmės pageidaujama, kad bendra peržiūra apimtų ne tik susitikimus su JAV agentūrų, organizacijų ir verslo atstovais, bet ir tam tikrų „privatumo skydo“ elementų patikrinimus vietoje. Bendroje peržiūroje DAI atstovai turėtų galėti teikti rekomendacijas dėl tokių patikrinimų vietoje.

DG29 mano, kad bendrai peržiūrai būtinas bendras rezultatų įvertinimas. Galiausiai bendrų peržiūrų rezultatai buvo pateikti Komisijos tarnybų dokumente, kuriam nebuvo būtinas ne Komisijos bendros peržiūros komandos narių patvirtinimas. DG29 pageidautų, kad bendros „privatumo skydo“ peržiūros ataskaita apie rezultatus iš tikrųjų būtų bendras produktas. Priešingu atveju gali būti svarstomas atskiros DAI ataskaitos apie bendrą peržiūrą sudarymas.

Galiausiai, bendros peržiūros atžvilgiu DG29 primena Komisijos pažadą, kad DG29 atstovų bendrųjų peržiūrų metu patirtos išlaidos būtų kompensuojamos Komisijos. Darbo grupė daro prielaidą, kad tai taip pat galios bendrai „privatumo skydo“ peržiūrai, bet kokių atveju tam tikram DAI atstovų skaičiui.

DG29 rekomenduoja, kad vėliausiai likus trims mėnesiams iki pirmosios bendros „privatumo skydo“ peržiūros Komisija, JAV administracija ir DG29 suderintų bendros peržiūros sąlygas ir įformintų jas raštiškai.

1.2.4 Persvarstoma ES teisinė sistema

Sprendimas dėl „privatumo skydo“ tinkamumo yra pirmasis sprendimas dėl tinkamumo, kuris buvo sudarytas remiantis principiniu susitarimu dėl Bendrojo duomenų apsaugos reglamento teksto. Tačiau DG29 nustatė, kad „privatumo skydas“ kol kas neatspindi būsimos situacijos. Pavyzdžiui, svarbios naujos sąvokos, kaip teisė į duomenų perkeliamumą ir papildomi duomenų valdytojo įsipareigojimai, įskaitant poreikį atlikti duomenų apsaugos poveikio įvertinimus ir laikytis „pritaikytosios privatumo apsaugos“ ir „standartizuotosios privatumo apsaugos“ principų, nebuvo įtrauktos į „privatumo skydą“. Todėl DG29 siūlo, kad „privatumo skydas“, kaip ir esamų sprendimų dėl tinkamumo atveju, būtų peržiūrimas netrukus pradėjus taikyti BDAR. Būtų pageidautina aiški nuoroda į šį peržiūros procesą galutiniam sprendime dėl tinkamumo.

2. SPRENDIMO DĖL TINKAMUMO PROJEKTO KOMERCINĖS DALIES ĮVERTINIMAS

2.1. Bendrosios pastabos

2.1.1 Patobulinimai

DG29 palankiai vertina „privatumo skydo“ patobulinius ir derybininkų ketinimus pašalinti nustatytus „saugaus uosto“ trūkumus. Tiksliau, lyginant su „saugiu uostu“, patobulinti šie elementai: keleto pagrindinių apibrėžčių, pvz., „asmens duomenys“, „duomenų tvarkymas“ ir „tvarkytojas“, įterpimas, mechanizmų, skirtų užtikrinti „privatumo skydo“ sąrašo priežiūrą ir šiuo metu privalomą išorinę arba vidinę atitikties peržiūrą, nustatymas. Taip pat patobulintas Prieigos principas, ir DG29 pažymi, kad kai duomenys naudojami su „privatumo skydo“ principais nesuderinamu būdu, numatytos taisymo ir ištrynimo teisės. Be to, dabar aiškiai nurodoma, kad asmuo turi gauti patvirtinimą, kad duomenys apie jį tvarkomi, ir informaciją apie tvarkomus duomenis.

DG29 taip pat palankiai vertina teisinių garantijų įgyvendinimą, vykdamą tolesnį perdavimą, ir PD įsipareigojimus bei tai, kad Federalinė prekybos komisija (FPK) vykdo pagal „privatumo skydą“ numatytus įsipareigojimus.

2.1.2 „Privatumo skydo“ taikymas organizacijoms, kurios veikia kaip duomenų tvarkytojos (atstovės)

Deja, kol kas lieka neaišku, kokių mastu „privatumo skydo“ principai taikomi įgaliotoms organizacijoms, kurios gauna asmens duomenis iš ES vien duomenų tvarkymo tikslais (toliau – „atstovai“ arba „tvarkytojai“). II priedo III.10.a skirsnio nuostatose minimas duomenų perdavimas įgaliotoms organizacijoms tokiais tikslais – t. y. minimas reikalavimas sudaryti sutartį – jose nėra nurodyta, kaip „privatumo skydo“ principai taikomi duomenų tvarkytojams (atstovams). Dėl to atsiranda neapibrėžtumas dėl įgaliotų JAV organizacijų, kurios gauna

duomenis tvarkymo tikslais, ir ES bendrovių, vykdančių duomenų perdavimą įgaliotoms organizacijoms, kurios veikia kaip duomenų tvarkytojos, bei asmenų, kurių duomenys tvarkomi, atžvilgiu. Dėl to bus sudėtinga nustatyti, kokie įsipareigojimai faktiškai taikomi „skydo“ organizacijoms, kurios tvarko asmens duomenis, gautus iš ES, joms vykdančioms savo kaip duomenų tvarkytojų funkcijas. Todėl būtinas paaiškinimas.

Todėl turi būti atsižvelgta į tai, kad keli į Principus įtraukti įsipareigojimai netinkami duomenų tvarkytojams, kadangi duomenų tvarkymo tikslus ir priemones visada nustato duomenų tvarkytojas (žr. „duomenų tvarkytojo“ apibrėžtį II priedo I.8.c skirsnyje). Taip yra dėl to, kad kai kurie Principuose nurodyti įsipareigojimai, jeigu jie galioja kaip atstovei veikiančiai organizacijai, gali prieštarauti duomenų tvarkymo sutarčiai, kuri yra būtina pagal ES įstatymus (sutartis nurodyta II priedo III.10.a skirsnyje). Pavyzdžiui, pagal duomenų tvarkymo sutartį duomenų tvarkytojas (atstovas) iš esmės neįgaliojamas duomenis toliau perduoti trečiosios šalies duomenų valdytojui, netgi esant II priedo II.3.a skirsnyje nurodytoms aplinkybėms. Tolesnis perdavimas trečiosios šalies atstovams galimas tik gavus duomenų valdytojo patvirtinimą. Be to, remiantis ES įstatymų nuostatų reikalavimais, duomenų tvarkytojas (atstovas) negalės asmenims teikti išsamių pranešimų, kaip numatyta Pranešimo principu (II priedo II.1 skirsnis), pavyzdžiui, kadangi ši organizacija nenustato duomenų tvarkymo tikslų.

Todėl būtina Principuose išaiškinti, kad tokio prieštaravimo atveju pirmenybė bus teikiama duomenų tvarkymo sutarties nuostatomis ir ypač organizacijos, kuri perduoda duomenis iš ES, nurodymams. Be tokio paaiškinimo Principai gali būti aiškinami ir taikomi „skydo“ atstovui suteikiant per daug kontrolės galimybių, ir dėl to iškiltų rizika, kad ES duomenų eksportuotojas pažeis savo, kaip duomenų tvarkytojo, įsipareigojimus pagal ES duomenų apsaugos įstatymus, kurie galioja perduodant duomenis „skydo“ organizacijai, veikiančiai kaip atstovė. Be to, dėl aiškumo trūkumo susidaro įspūdis, kad duomenų tvarkytojas gali pakartotinai naudotis duomenimis pagal savo pageidavimus.

Be to, turi būti pateiktos konkrečios taisyklės, galiojančios, kai organizacija veikia kaip duomenų tvarkytoja (atstovė), siekiant užtikrinti, kad ši organizacija vykdytų duomenų tvarkytojo nurodymus. Turėtų būti aiškiai nurodyta, kad JAV organizacijos, kurios gauna duomenis tik tvarkymo tikslais, negali savo vardu nuspręsti tvarkyti duomenis. Jeigu nėra konkrečių taisyklių, kurios galioja organizacijoms, veikiančioms kaip duomenų tvarkytojos, sudėtinga nustatyti, kokias taisykles duomenų tvarkytojas (atstovas) pažeistų, jeigu galėtų atlikti autosertifikavimo procedūrą.

2.1.3 Įsipareigojimo laikyti Principų apribojimai

II priedo I.5 skirsnyje, be kita ko, nurodomos Principų išimtys, kai duomenys, kuriems galioja „privatumo skydas“, naudojami nacionalinio saugumo¹², viešųjų interesų, teisėsaugos tikslais arba pagal statutą, vyriausybės nutarimus ar teismų praktiką, dėl ko atsiranda prieštaringi įsipareigojimai ar aiškūs įgaliojimai. Neturint išsamių žinių apie JAV įstatymus tiek

¹² Daugiau komentarų apie asmens duomenų, kuriems galioja „privatumo skydas“, naudojimą nacionalinio saugumo tikslais pateikta 3 skyriuje, o teisėsaugos tikslais – 4 skyriuje.

federaliniu, tiek valstybiniu lygmeniu, DG29 sudėtinga įvertinti šios išimties apimtis ir nuspręsti, ar šie apribojimai pateisinami demokratinėje visuomenėje. Būtų labai svarbu, kad Europos Komisija į sprendimo dėl tinkamumo projektą įtrauktų apsaugos lygio analizę, kuriai galiotų tos išimtys. DG29 ragina Komisiją užtikrinti, kad ES būtų informuota apie bet kokius įstatymus ar vyriausybės nutarimus, kurie paveiktų šiuo metu taikomų arba naujų įstatymų ar nutarimų įsigaliojimo JAV metu galiosiančių principų laikymąsi.

2.1.4 Duomenų saugojimo apribojimų principo trūkumas

Duomenų saugojimo apribojimų principas (direktyvos 6 straipsnio 1 dalies e punktas) yra pagrindinis ES duomenų apsaugos įstatymo principas, kuriuo nustatoma, kad asmeniniai duomenys turi būti saugomi tiek, kiek reikia, siekiant tikslo, dėl kurio buvo renkami duomenys arba dėl kurio jie toliau tvarkomi.

Tačiau DG29 „privataus skydo“ dokumentuose negali rasti nuorodos, kad duomenų valdytojai privalo užtikrinti, jog duomenys būtų pašalinti nebelikus tikslo, dėl kurio jie buvo renkami arba toliau tvarkomi. Taigi, atrodo, kad Principuose sertifikuotoms organizacijoms nenumatyta duomenų saugojimo laikotarpio apribojimų, kurie taikomi pagal ES įstatymuose reglamentuotą duomenų saugojimo apribojimų principą.

Duomenų vientisumo ir tikslo ribojimo principo formuluotė (II priedo II.5 skirsnis) jokių būdu negali būti traktuojama kaip sukurianti organizacijos, kuri veikia kaip duomenų valdytoja, įsipareigojimą pašalinti duomenis, kai jie tampa nebereikalingi tais tikslais, kuriais jie buvo renkami ar toliau tvarkomi, arba organizacijos, kuri veikia kaip duomenų tvarkytoja, įsipareigojimą pašalinti duomenis, nutraukus paslaugų sutartį.

Darbo grupė pabrėžia, kad tai, jog nėra nuostatų, pagal kurias ribojamas duomenų saugojimas pagal „privatumo skydą“, organizacijoms suteikia galimybę saugoti duomenis tiek, kiek jos pageidauja, netgi kai nebegalioja „privatumo skydo“ nuostatos, o tai prieštarauja esminiam duomenų saugojimo apribojimų principui.

2.1.5 Automatizuotų sprendimų garantijų trūkumas, dėl kurio kyla teisinės pasekmės arba labai pakenkiama asmeniui

„Privatumo skydas“ neužtikrina jokių teisinių garantijų, jeigu asmens atžvilgiu priimamas sprendimas, kuris sukuria su juo susijusias arba labai jam pakenkiančias teises pasekmes ir kuris yra paremtas tikrai automatizuotu duomenų tvarkymu, skirtu įvertinti tam tikrus asmeniškumus su juo susijusius aspektus, kaip antai: jo darbo rezultatai, kreditingumas, patikimumas, elgesys ir kt.

Būtinybę teikti teisėtas garantijas automatizuotiems sprendimams (kurie sukelia teises pasekmes ar labai paveikia asmenį), siekiant užtikrinti atitinkamą apsaugos lygį, jau pabrėžė DG29 savo 12 darbo dokumente.

Tai tampa vis svarbiau, kadangi nuolat tobulinamos naujosios technologijos daugiau bendrovių sudaro sąlygas svarstyti automatizuotų sprendimų priėmimo sistemų diegimą, dėl

ko gali pablogėti žmonių, paliktų be teisės užginčyti tuos kompiuterių priimtus sprendimus, padėtis. Kadangi tik tų automatizuotų sistemų priimti sprendimai daro įtaką asmenų teisei situacijai arba gali labai jiems pakenkti (pavyzdžiui, įtraukiant į juodąjį sąrašą ir atimant atitinkamas teises), labai svarbu užtikrinti pakankamas apsaugos priemones, įskaitant teisę žinoti taikomą logiką ir reikalauti persvarstymo neautomatiniu būdu.

2.1.6 Esamų komercinių santykių tarpinis laikotarpis

„Privatumo skydo“ sąlygose numatoma, kad Principai įsigalioja nedelsiant po sertifikavimo. Tačiau organizacijos, kurios atliks sertifikavimo procedūras per pirmuosius du mėnesius nuo „privatumo skydo“ sistemos įsigaliojimo, turės kuo greičiau suderinti esamus komercinius santykius su trečiosiomis šalimis, atsižvelgiant į atskaitomybę už tolesnio perdavimo principą. Bet kokių atveju jos turi tai padaryti ne vėliau nei praėjus devyniems mėnesiams nuo dienos, kai jos sertifikuojasi pagal „privatumo skydą“.

Tai reiškia, kad esamos sutartys, kiek tai būtina, turi būti suderintos su Principais per du–devynis mėnesius nuo sertifikavimo. Šiuo tarpiniu laikotarpiu pakanka pranešimo ir pasirinkimo. DG29 pabrėžia tai, kad perdavimas gali būti vykdomas „privatumo skydo“ pagrindu tik nuo to momento, kai organizacija visiškai įvykdo visus „skydo“ reikalavimus. Negali būti laikoma, kad galimybė nusiųsti duomenis tarpiniu laikotarpiu, kai gavėjas ne visiškai atitinka „skydo“ reikalavimus, atitinka perdavimo pagal teisės nuostatas sąlygas, todėl ši galimybė nėra priimtina.

2.2. Kitos pastabos

2.2.1 Skaidrumas

a) Bendros pastabos dėl pranešimo

DG29 palankiai vertina tai, kad išsamesni reikalavimai yra išdėstyti Pranešimo principu, visų pirma tai, kad pranešime turės būti pateikta nuoroda į „privatumo skydo“ sąrašą arba turės būti pateiktas „privatumo skydo“ sąrašo internetinis adresas ir nurodytos asmenų prieigos teisės bei alternatyvūs ginčų sprendimo būdai¹³. Tačiau DG29 rekomenduoja tiksliau nurodyti kitas teises (taisyti, ištrinti, jeigu netiksliai nurodyta arba tvarkoma pažeidžiant Principus).

„Privatumo skydą“ sudarantys dokumentai kelia susirūpinimą dėl laiko, kada „privatumo skydo“ organizacija turi pateikti pranešimą asmeniui. II priedo II.1.b punkte nurodoma, kad „pranešimas turi būti pateiktas (...), kai asmenų pirmą kartą prašoma suteikti asmeninę informaciją organizacijai arba kiek įmanoma greičiau po to, tačiau bet kuriuo atveju prieš organizacijai panaudojant tokią informaciją kitais tikslais, nei tie, dėl kurių duomenis perduodančioji organizacija ją iš pradžių surinko ar tvarkė, arba prieš pirmą kartą ją atskleidžiant trečiajai šaliai“. DG29 mano, kad daugelyje situacijų JAV „skydo“ organizacija tiesiogiai nerinks duomenų iš duomenų subjekto, taigi pranešimas turi būti teikiamas, kai duomenis įrašo „skydo“ organizacija.

¹³ II priedo II.1 skirsnis; DG29 taip pat mini antrąją Komisijos rekomendaciją, pateiktą Komunikate COM(2103)847 bei 2014 m. balandžio 10 d. DG 29 rašte pirmininko pavaduotojai V. Reding, tiksliau, skyriaus „Skaidrumas“ 4 punktą.

DG29 pažymi, kad faktinis reikalavimų įgyvendinimas, atsižvelgiant į pranešimo principą ir privatumo politiką, turėtų būti įvertintas pirmoje metinėje „privatumo skydo“ peržiūroje.

b) Privatumo politikos viešas prieinamumas

DG29 palankiai vertina faktą, kad dabar yra aišku, jog PD patikrins, ar bendrovės, kurios turi viešuosius tinklalapius, juose paskelbė savo privatumo politiką arba, jeigu jos neturi viešųjų tinklalapių, kur jos skelbia privatumo politiką¹⁴.

c) Sutarčių su duomenų tvarkytojais privatumo sąlygų paskelbimas

Be sąlygų, kuriomis „privatumo skydo“ organizacijos gali perduoti duomenis duomenų tvarkytojui (atstovui), „privatumo skydo“ nuostatose numatoma, kad autosertifikuotos organizacijos įsipareigoja „pateikti su tuo atstovu sudarytos sutarties privatumo nuostatų santrauką ar kopiją, Departamentui pareikalavus“ (žr. II priedo II. 3.b.v skirsnį). Darbo grupė palankiai vertina šį PD taikomą skaidrumo reikalavimą.

2.2.2 Pasirinkimas

Pagal „privatumo skydo“ nuostatas suteikiama teisė pasirinkti atskleisti asmeninę informaciją trečiosioms šalims arba asmens informaciją naudoti visiškai kitais tikslais¹⁵ (II priedo III.2 skirsnis). Be to, asmenys gali pasinaudoti „pasirinkimo“ teise asmeninę informaciją bet kuriuo metu naudoti tiesioginės rinkodaros tikslais (II priedo III.12.a skirsnis)¹⁶.

Išskyrus tuos atvejus, kai tai būtina tiesioginės rinkodaros tikslais, duomenys apie šio pasirinkimo būdą ir momentą nepateikiami. DG29 mano, kad paprasta nuoroda į šios teisės egzistavimą privatumo politikoje negali būti pakankama – turėtų būti pasiūlyta *individualizuota* galimybė pasinaudoti šia teise *prieš* atskleidžiant ar pakartotinai naudojant asmeninę informaciją.

Be to, DG29 pabrėžia, kad „privatumo skydo“ nuostatose turi būti numatyta bendra teisė atšaukti (dėl įtikinamų pagrindų, susijusių su konkrečia duomenų subjekto situacija), suprantama kaip teisė paprašyti nutraukti duomenų tvarkymą, kai asmuo turi įtikinamų teisėtų priežasčių, susijusių su konkrečia situacija¹⁷. DG29 primygtinai rekomenduoja, kad sprendimo dėl tinkamumo projekte būtų aiškiai nurodyta, jog teisė atšaukti turėtų egzistuoti bet kuriuo momentu ir kad šis atšaukimas neapsiriboja duomenų naudojimu tiesioginės rinkodaros tikslais¹⁸.

DG29 nuogąstauja, kad apibrėžties, kas yra „iš esmės kitoks tikslas“, trūkumas sukels painiavą ir teisinį neapibrėžtumą. Reikėtų paaiškinti, kad bet koku atveju Pasirinkimo

¹⁴ Žr. pirmąją Europos Komisijos rekomendaciją komunikate COM(2013)847 ir 2014 m. balandžio 10 d. DG29 raštą pirmininko pavaduotojai V. Reding, ypač skyriaus „Skaidrumas“ 3 punktą.

¹⁵ Papildomame principo 14.c.I numatoma teisė nebedalyvauti klinikiniame tyrime, kuri gali būti laikoma teise atšaukti arba panaikinti sutikimą.

¹⁶ Ši sąlyga yra tokia pati, kaip ir buvo nurodyta „saugaus uosto“ sistemoje (DUK 12), ir šiuo atžvilgiu nebuvo atlikta jokių pakeitimų.

¹⁸ Žr. DG29 raštą pirmininko pavaduotojai V. Reding, skyrių „Pasirinkimas“.

principas negali būti taikomas, siekiant apeiti Tikslų ribojimo principo reikalavimus¹⁹. Pasirinkimas turėtų būti galimas, tik jeigu tikslas iš esmės skiriasi, tačiau yra suderinamas, kadangi duomenų tvarkymas nesuderinamais tikslais yra draudžiamas (II priedo II.5.a skirsnis). Reikia patikslinti, kad teisė pasirinkti organizacijai negali sudaryti galimybių naudoti duomenų nesuderinamais tikslais. Taigi, rekomenduojama suderinti susijusią formuluotę, naudojant vieningą ir apibrėžtą formuluotę (pvz., „iš esmės kitoks, bet nepaisant to suderinamas tikslas“).

Būtų naudingas paaiškinimas, kada sprendimui duomenis tvarkyti kitu tikslu arba atskleisti informaciją galioja ES įstatymai. Šioje situacijoje duomenų tvarkymui tiesiogiai galioja įprastinės ES teisinės sąlygos (pvz., draudimas tvarkyti duomenis nesuderinamais tikslais, pateikti teisėtus duomenų tvarkymo pagrindus ir būtinybė informuoti asmenį), įskaitant JAV organizacijas, kurioms taikomi ES įstatymai. Praktiškai tai reiškia, kad ES eksportuotojas, kuris priima tokį sprendimą, turėtų užtikrinti duomenų tvarkymo skaidrumą ir teisėtumą pagal ES įstatymus. Todėl pasirinkimo principas galios tik tuo atveju, jeigu sprendimas priimamas išskirtinai JAV „skydo“ organizacijos, kuriai negalioja ES įstatymai.

2.2.3 Tolesnis perdavimas

a) Taikymo sritis

DG29 nerimauja dėl situacijos, kai asmens duomenys perduodami toliau iš „privatumo skydo“ organizacijos JAV gavėjui trečiojoje šalyje.

„Skydas“ turėtų būti laikomas ne tik įrankiu, skirtu perkelti ES duomenis iš ES į JAV, tačiau taip pat pasitarnaus kaip įrankis perduoti duomenis iš JAV trečiosioms šalims. Todėl tolesnio perdavimo nuostatos yra svarbus „skydo“ elementas, kuris turėtų užtikrinti pakankamas garantijas ir atitinkamą apsaugos lygį, kai duomenys toliau perduodami už JAV ribų. Vienas konkretus klausimas yra susijęs su nacionaliniu saugumu ir teisėsauga.

Atskaitomybė už „privatumo skydo“ tolesnių perdavimų principą neapsiriboja gavėjų duomenų valdytojais, tvarkytojais ar atstovais, įsteigtais JAV. Todėl tolesni perdavimai į trečiąją šalį gali būti vykdomi „privatumo skydo“ pagrindu, netgi jeigu trečiojoje šalyje galioja įstatymai, reglamentuojantys viešą prieigą prie asmens duomenų, pavyzdžiui, stebėjimo tikslais. Dėl to iškyla nepateisinamo kišimosi į pagrindines teises grėsmė.

Tolesnio perdavimo į trečiąją šalį atveju visos „privatumo skydo“ organizacijos turėtų būti įsipareigojusios įvertinti duomenų importuotojui taikomus būtinus trečiosios šalies nacionalinių įstatymų reikalavimus prieš perdavimą. Jeigu nustatoma iš esmės neigiamo poveikio „privatumo skydo“ suteiktoms garantijoms, įsipareigojimams ir apsaugos lygiui rizika, JAV „privatumo skydo“ organizacija, veikianti kaip duomenų tvarkytoja (atstovė), prieš atlikdama bet kokius tolesnius perdavimus privalės nedelsdama informuoti ES duomenų valdytoją. Šiais atvejais duomenų eksportuotojas turi teisę sustabdyti duomenų perdavimą ir

¹⁹ Tikslus tolesnio nesuderinamo duomenų tvarkymo, leistino pagal Pasirinkimo principą, pavyzdys pateiktas Papildomame principo 9.b.i (žr. DG29 komentarą apie tai straipsnyje apie „žmogiškųjų išteklių duomenis“).

(arba) nutraukti sutartį. Jeigu išskyla didelio neigiamo poveikio rizika, „skydo“ organizacijai, kuri veikia kaip duomenų valdytoja, neturėtų būti leidžiama toliau perduoti duomenis, kadangi tai galėtų neigiamai paveikti jos pareigą užtikrinti tą patį apsaugos lygį kaip ir pagal Principus tolesnių perdavimų atveju (žr. II priedo II.3.a skirsnį).

Panašiai, jeigu pakeičiami trečiosios šalies įstatymai ir tai gali iš esmės neigiamai paveikti „privatumo skydo“ suteiktas garantijas, įsipareigojimus ir apsaugos lygį, JAV „privatumo skydo“ organizacija, veikianti kaip duomenų tvarkytoja (atstovė), turėtų būti įpareigota – „privatumo skydo“ pagrindu – nedelsdama pranešti apie šį pakeitimą duomenų eksportuotojui, kai tik ji sužino apie tai, kokių atveju duomenų eksportuotojas turi teisę sustabdyti duomenų perdavimą ir (arba) nutraukti sutartį. Atitinkamai, „skydo“ organizacijai, veikiančiai kaip valdytojai, neturėtų būti leidžiama duomenis perduoti toliau, kadangi ji privalo užtikrinti tą patį apsaugos lygį kaip ir pagal Principus (žr. II priedo II.3.a skirsnis).

DG29 primena savo poziciją, kad jeigu ES duomenų valdytojas žino apie tolesnį perdavimą trečiajai šaliai už JAV ribų dar prieš perdavimą JAV arba jeigu ES duomenų valdytojas yra bendrai atsakingas už sprendimą leisti toliau perduoti duomenis, perdavimas turėtų būti laikomas tiesioginiu perdavimu iš ES trečiajai šaliai už JAV ribų. Tai reiškia, kad vietoje „privatumo skydo“ tolesnio perdavimo principo perdavimui taikomi direktyvos 25 ir 26 straipsniai.

b) Perdavimai iš „privatumo skydo“ organizacijos trečiosios šalies valdytojui

DG29 palankiai vertina pareigą taikyti sutartis (II priedo II.3.a skirsnis), siekiant užtikrinti, kad trečiosios šalies duomenų valdytojas užtikrins bent tokį patį privatumo apsaugos lygį, koks reikalaujamas pagal „privatumo skydo“ principus. Tikslas yra užtikrinti, kad asmens duomenys ir toliau būtų atitinkamai saugomi, netgi juos perdavus toliau. Tačiau DG29 turi kelias pastabas dėl siūlomų sąlygų.

Nuorodos į Tikslą ribojimo principą trūkumas

DG29 taip pat rekomenduoja į tolesnio perdavimo trečiosios šalies duomenų valdytojui sąlygas (II priedo II.3.a skirsnis) įtraukti aiškią nuorodą į Tikslą ribojimo principą (II priedo II.5 skirsnis). Tokiu būdu būtų aiškiai nustatyta, kad tolesni perdavimai negali būti vykdomi, kai trečiosios šalies duomenų valdytojas apdoroja duomenis nesuderinamais tikslais.

Sutarties dėl perdavimų grupės viduje tarp valdytojų reikalavimo išimtis

Sutarties reikalavimo išimtis numatyta perdavimams tarp valdytojų grupės viduje. Pagal tokį scenarijų Principuose nurodyta, kad apsaugos tęstinumas gali būti numatytas įmonei privalomose taisyklėse (IPT) arba „kitose priemonėse grupės viduje (pvz., atitikties ir kontrolės programose)“ (II priedo III.10.b skirsnis). DG29 mano, kad nuoroda į „kitas priemones grupės viduje“ negarantuoja kitų grupės narių pagal teisės nuostatas įpareigojančių

įsipareigojimų. Kadangi DG29 nuomone ir pagal ES teisės aktus²⁰ iš esmės teigiamai vertinami įpareigojantys įsipareigojimai sudaryti perdavimus grupės viduje, svarbu užtikrinti, kad „privatumo skydas“ nebūtų naudojamas šiam reikalavimui apeiti. DG29 primena, kad bet kokių atveju tolesni perdavimai iš JAV trečiosioms šalims, planuojami dar prieš perdavimą į JAV arba bendrai valdomi su ES duomenų valdytoju²¹, turi būti laikomi tiesioginiu perdavimu iš ES į trečiąją šalį už JAV ribų. Todėl perdavimui galioja direktyvos 25 ir 26 straipsniai.

c) Perdavimai iš „privatumo skydo“ organizacijos trečiosios šalies duomenų valdytojui (atstovui)

DG29 palankiai vertina faktą, kad sutartis dėl tolesnių perdavimų dabar privaloma duomenis gaunantiems subjektams, kurie veikia kaip duomenų tvarkytojai (atstovai), nepaisant jų dalyvavimo „privatumo skyde“ arba to, kad jie naudojami kitu tinkamumo nustatymo sprendimu. DG29 taip pat palankiai vertina papildomas apsaugos priemones, reglamentuojant tuos tolesnius perdavimus (II priedo II.3.a.i; II.3.a.iii; II.3.a.iv; II.3.a.v; II.7.d skirsnis). Paskutiniame punkte (II priedo II.7.d skirsnis) apibrėžiamas įsipareigojimas išlikti atsakingu, kai duomenys atskleidžiami atstovui. Tačiau atrodo, kad ši garantija negalios tais atvejais, jeigu organizacija nusprendė bendradarbiauti su DAI (žr. II priedo III.5.a skirsnį). DG29 nesupranta tokios išimties priežasties ir mano, kad netgi šiuo atveju atsakomybė turėtų būti taikoma.

Nuorodos į Tikslų ribojimo principą trūkumas

DG29 pažymi, kad Atskaitomybės už tolesnį perdavimą principu (II priedo II.3 skirsnis) paaiškinama, kad asmens duomenys gali būti perduoti trečiajai šaliai, kuri veikia kaip atstovė, tik ribotais ir nurodytais tikslais, tačiau aiškiai nenurodyta, kad šie riboti ir nurodyti tikslai turi būti suderinami su pradiniais tikslais, kuriais duomenys buvo surinkti, bei su duomenų valdytojo nurodymais. Šiuo klausimu reikia daugiau aiškumo. Todėl DG29 rekomenduoja užtikrinti, kad sprendimas dėl tinkamumo būtų išsamesnis, pavyzdžiui, įterpiant aiškią nuorodą į Tikslų ribojimo principą (II priedo II.5 skirsnis), kuriuo remiantis duomenys negali būti tvarkomi (įskaitant atskleistus duomenis) nesuderinamais tikslais, vadovaujantis Tolesnio perdavimo principu (papildomai prie Pasirinkimo principo).

Daugiau papildomų „privatumo skydo“ organizacijų, kurios veikia kaip duomenų tvarkytojos (atstovės), įsipareigojimų, susijusių su duomenų perdavimu kitam duomenų tvarkytojui (atstovui), poreikis

Aiškių taisyklių trūkumas tuo atveju, kai „skydo“ organizacija veikia kaip atstovė (t. y. ES duomenų valdytojo vardu), yra akivaizdi spraga ir gali kliudyti ES duomenų valdytojui vykdyti valdymo funkcijas. „Skydo“ organizacija, kuri gauna duomenis kaip ES duomenų valdytojo atstovė, turi vykdyti ES valdytojo nurodymus. Tai turėtų būti aiškiai nurodyta

²⁰ Įpareigojančių ir įgyvendinamų įsipareigojimų būtinybė taip pat pabrėžiama BDAR, nepriklausomai nuo to, koks įrankis naudojamas (IPT, sutartinės nuostatos, elgesio kodeksai arba sertifikavimas).

²¹ Pavyzdžiui, žmoniškųjų išteklių duomenims.

Principuose, siekiant užtikrinti, kad tų nurodymų nepaisymas būtų laikomas ne tik sutarties (II priedo III.10.a.ii skirsnis), bet ir „privatumo skydo“ principų pažeidimu.

Galimybė „skydo“ organizacijai, kuri veikia kaip atstovė, vėliau perduoti duomenis trečiosios šalies atstovui turi būti skaidri duomenų valdytojui ir turi būti iš anksto patvirtinta. Todėl turi būti aiškiai nurodyta, kad tai yra atstovo su ES duomenų valdytoju pasirašyta sutartis (nurodyta 10 DUK kaip „17 straipsnio sutartis“), kurioje numatyta, ar leidžiamas tolesnis perdavimas.²²

Esamos tolesniam perdavimui atstovui galiojančios sąlygos yra pagrįstos prielaida, kad „skydo“ organizacija veikia kaip valdytoja ir todėl gali savarankiškai priimti sprendimą dėl galimos trečiosios šalies atstovo intervencijos. Tačiau tai nebūtų įmanoma, kai „skydo“ organizacija veikia kaip atstovė. Priešingu atveju iš ES valdytojo bus atimti valdymo įgaliojimai.

Susijusios su trečiosios šalies atstovu sudarytos sutarties privatumo nuostatos turi būti perduotos valdytojui ir turi užtikrinti bent tokį patį apsaugos lygį, kaip nurodyta su duomenų valdytoju pasirašytoje sutartyje.

2.2.4 Duomenų vientisumas ir tikslo ribojimas

a) Proporcingumo principas

DG29 primena apie savo raštą pirmininko pavaduotojai V. Reding, kuriame rašė, kad „netgi griežtai laikantis Pranešimo ir Pasirinkimo principų, asmens duomenys gali būti tvarkomi neproporcingai su duomenų subjekto ar visuomenės interesais susijusių teisių ir laisvių atžvilgiu. Proporcingumo ar protingumo principų turi būti laikomasi visuose duomenų tvarkymo etapuose ir jais turi būti vadovaujamasi papildomai prie Pranešimo ir Pasirinkimo principų“²³.

„Privatumo skydo“ nuostatose (II priedo II.5.a skirsnis) numatyta, kad turi būti apsiribota duomenų tvarkymui svarbia informacija. DG29 pageidautų, kad ši formuluotė galutiniame sprendime dėl tinkamumo būtų pakeista, kadangi vien to, kad duomenys yra susiję su duomenų tvarkymu, nepakanka, norint užtikrinti duomenų tvarkymo proporcingumą. Siekiant laikytis proporcingumo principo, tvarkymas turėtų apsiriboti duomenimis, kurie reikalingi būtinam duomenų tvarkymui.

b) Tikslumas

Pagal duomenų vientisumo ir tikslo ribojimo principą (II priedo II.5 skirsnis) taip pat numatoma: „Tiek, kiek būtina tokiems tikslams, organizacija turi imtis pagrįstų priemonių, siekdama užtikrinti, kad asmens duomenys atitiktų numatomą jų naudojimo paskirtį, būtų tikslūs, išsamūs ir galiojantys“. DG29 pažymi, kad tai yra lygiai tokia pati formuluotė, kokia naudojama „saugaus uosto“ susitarime. DG29 abejoja, ar turėtų būti įtraukta formuluotė „kiek

²² Žr. DG29 raštą pirmininko pavaduotojai V. Reding, 2014 m. balandžio 10 d., skyriaus apie tolesnį perdavimą 4 punktas.

²³ Žr. DG29 raštą pirmininko pavaduotojai V. Reding, 2014 m. balandžio 10 d., 8 p.

tai būtina šiais tikslais“, kadangi jos požiūriu, duomenų tikslumas neturėtų priklausyti nuo duomenų tvarkymo tikslo. DG29 pageidautų, kad galutiniame sprendime dėl tinkamumo ši sąsaja nebūtų nurodoma.

c) Tikslo apribojimas

Jeigu asmens duomenys perduodami JAV organizacijai ES įsteigto duomenų valdytojo, duomenų eksportuotojas turėtų tiksliai informuoti JAV organizaciją apie tikslus, kuriais iš pradžių buvo renkami duomenys. Tai būtina siekiant nustatyti, ar po perdavimo tikslas pakeičiamas; tokiu būdu pritaikomi Pranešimo ir Pasirinkimo principai ir prisidedama prie rizikos ir atsakomybės priskyrimo.

Pagal Duomenų vientisumo ir tikslo ribojimo principą (II priedo II.5 skirsnis) nurodoma, kad organizacija negali tvarkyti asmeninės informacijos, jeigu tikslai neatitinka tikslų, dėl kurių ji buvo iš pradžių surinkta ar vėliau buvo gautas asmens sutikimas ją naudoti. Tačiau pagal Pasirinkimo principą (II priedo II.2 skirsnis) numatomas pasirinkimas „naudoti“ slaptą informaciją (t. y. asmeninę informaciją, apibrėžiančią medicininę ar sveikatos būklę, rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narysę profesinėse sąjungose arba informaciją apie asmens lytinį gyvenimą bei duomenis apie teistumą) tikslais, kurie iš esmės skiriasi nuo tikslų, kuriais duomenys iš pradžių buvo renkami ar kuriuos naudoti asmuo vėliau davė savo sutikimą. Šis pasirinkimas nereikalaujamas 1.a papildomo principo atveju (II priedo III.1.a skirsnis). Jeigu asmeninė informacija yra neslapta, taikomas pasirinkimo principas.

DG29 pažymi, kad Tikslo ribojimo principo apimtis skiriasi Pranešimo, Pasirinkimo bei Duomenų vientisumo ir tikslo ribojimo principų atveju. Faktiškai tame pačiame tekste naudojami terminai „nesuderinamas tikslas“ ir „iš esmės kitoks tikslas“ be aiškaus šių sąvokų apibrėžimo²⁴.

DG29 rimtai susirūpinusi faktu, kad toks nenuoseklumas gali sukelti didelių sunkumų Duomenų nuoseklumo ir tikslo ribojimo principą (II priedo II.5 skirsnis) suderinant su Pasirinkimo principu (II priedo II.2 skirsnis), kadangi vienas nustato, jog duomenys negali būti tvarkomi tais tikslais, kuriais jie buvo renkami, nesuderinamu būdu, tuo tarpu kitas nustato atsisakymo mechanizmą, jeigu duomenys tvarkomi tikslais, kurie iš esmės skiriasi nuo pradinio tikslo.

Taigi, Pasirinkimo principas gali būti laikomas įgalinančiu tolesnį nesuderinamą duomenų tvarkymą²⁵. DG29 teigimu, reikėtų aiškiai nurodyti, kad organizacija negalės tvarkyti duomenų iš esmės kitokiais tikslais, jeigu jie nesuderinami pagal Tikslo ribojimo principą. Kitaip tariant, turėtų būti aišku, kad Pasirinkimo principas nėra tikslo ribojimo išimtis.

²⁴ DG29 pažymėjo, kad taip pat naudojami kai kurie kiti išsireiškimai: „naudojama nesuderinamai su“ (II priedo III.14.b.ii skirsnis), „naudojama kitokiais tikslais“ (II priedo III. 9.B.i skirsnis), „naudojama ne tuo tikslu, kuriuo jie buvo renkami iš pradžių“ (II priedo II.1.b skirsnis). Dėl šio neaiškumo gali nebebūti suteikiama pakankamai garantijų tikslo ribojimo principo atžvilgiu.

²⁵ Taip pat žr. komentarą apie Pasirinkimo principą. DG29 mano, kad dėl to, jog tolesnio perdavimo taisyklės (II priedo II.3 skirsnis) taikomos tik Pasirinkimo principui, tačiau netaikomos Tikslo ribojimo principui, padidėja tokio supratimo rizika.

Bet kokių atvejų, jeigu tolesnis duomenų tvarkymas gali būti laikomas suderinamu, taip pat turėtų galioti Pranešimo ir Pasirinkimo principas.

2.2.5 Su žurnalistika susijusios išimtys

Su žurnalistika susijusios asmens duomenų tvarkymo išimtys numatytos 2 papildomame principu (II priedo III.2 skirsnis). Suprantama, kad šios nuostatos atspindi JAV žodžio laisvės konstitucinę apsaugą. Todėl „privatumo skydo“ dokumentuose nurodyta, kad „asmeninei informacijai, kuri yra surinkta skelbti, taip pat iš žurnalistikos archyvų anksčiau skelbtai informacijai, „privatumo skydo“ principų reikalavimai negalioja“ (II priedo III.2.b skirsnis). Ši išimtis taip pat galioja tolesniam duomenų valdytojo ar tvarkytojo duomenų tvarkymui, t. y. neapsiribojama tolesniu duomenų tvarkymu žurnalistiniais tikslais. Kaip nurodyta 2014 m. balandžio 10 d. rašte pirmininko pavaduotojai V. Reding, DG29 būtų pageidavusi labiau riboto požiūrio į su žurnalistika susijusias išimtis, labiau suderinamo su ES taikomu principu, kaip ir pašalinimo iš sąrašo teise, vadovaujantis *Google Spain* byla²⁶.

2.2.5 Duomenų subjektų prieigos, taisymo ir ištrynimo teisė

Remiantis „privatumo skydo“ nuostatomis, asmenys turi teisę gauti *patvirtinimą*, ar jų duomenys tvarkomi organizacijos, ir kad tokie duomenys būtų *perduoti jiems* (II priedo III.8.a.i skirsnis). Tačiau organizacijų įsipareigojimas atsakyti į asmenų užklausas dėl duomenų tvarkymo tikslų, susijusių asmens duomenų kategorijų ir gavėjų, kuriems atskleidžiami asmeniniai duomenys, ar jų kategorijų yra gana silpnas. DG29 mano, kad duomenų subjektui pateikti duomenys turi būti paminėti tekste, o ne išnašoje, ir jie turi būti suformuluoti kaip aiški prievolė (susijusi su II priedo III.8.a.i.1 skirsniu).

Remiantis 8 papildomu principu, „prieiga turi būti užtikrinta tik tiek, kiek organizacija saugo asmeninę informaciją“ (II priedo III.8.d.ii skirsnis). Ši taisyklė neturėtų būti griežtai taikoma ta prasme, kad iš esmės turi būti užtikrinta prieiga prie duomenų, kurie tvarkomi, o ne tik saugomi organizacijos. Todėl prieigos teisės efektyvumo tikslais svarbu užtikrinti, kad „saugomi“ reikštų „tvarkomi“, remiantis II priedo I.8.b skirsnyje pateikta apibrėžtimi. Šios taisyklės taikymas turi būti atidžiai išnagrinėtas bendros „privatumo skydo“ peržiūros metu.

Išlieka abejonių dėl išimčių sąrašo, pateikto II priedo III.8.e(i) skirsnyje, kuris yra panašus į pateiktą 8 „saugaus uosto“ DUK ir kuris turėtų užtikrinti geresnę organizacijų interesų apsaugą. Šiuo atžvilgiu prieiga prie asmeninių duomenų nebus suteikta asmenims dėl šių priežasčių: „profesinių lengvatų ar įsipareigojimų pažeidimas“ (II priedo III.8.e.3 skirsnis), „kenkimas darbuotojo saugos tyrimui ar skundų procedūrai, arba dėl darbuotojų pareigų perėmimo ir įmonių reorganizavimo“ (II priedo III.8.e.4 skirsnis) ir „pakenkimas konfidencialumui, kuris gali būti būtinas stebėsenos, tikrinimo ar kontrolės funkcijoms, susijusioms su patikimu valdymu, arba ateityje vyksiančioms ar vykstančioms deryboms, kuriose dalyvauja organizacija“ (II priedo III.8.e.5 skirsnis). Į šias priežastis reikėtų

²⁶ 2014 m. gegužės 13 d. sprendimas byloje *Google Spain / Agencia Española de Protección de Datos and Mario Costeja González*, C-131/12,

atsižvelgti papildomai prie bendros išimties dėl konfidencialios komercinės informacijos, kuri įtraukta į II priedo III.8.c skirsnį. Todėl asmuo niekada neturės prieigos prie savo duomenų pirmiau nurodytais atvejais, nebus asmens ir organizacijos, kurie siekia sprendimo dėl prieigos prašymo, teisių ir interesų pusiausvyros.

DG29 primena, kad prieigos prie savo duomenų teisė suteikiama asmenims, nurodytiems Chartijos 8 straipsnio 2 dalyje. Nors tai nėra absoliuti teisė, ji ypač svarbi teisei į asmens duomenų apsaugą, kadangi taip supaprastinamas naudojimasis kitomis duomenų subjekto teisėmis, pavyzdžiui, teise taisyti ir ištrinti duomenis.

Kalbant apie teises taisyti ir ištrinti duomenis, DG29 palankiai vertina žymų patobulinimą, užtikrinantą „privatumo skydo“ principų, lyginant su „saugaus uosto“ principais, pagal kuriuos tos teisės suteikiamos ne tik tais atvejais, kai duomenys yra netikslūs, bet ir kai duomenys tvarkomi pažeidžiant principus (II priedo II.6 skirsnis).

2.2.6 Teisių gynimas, reikalavimų užtikrinimas ir atsakomybė (teisių gynimo mechanizmai)

a) Veiksmingas naudojimasis ES asmenų teisėmis į teisių gynimo priemones

DG29 pripažįsta JAV valdžios įstaigų įsipareigojimus įvairių teisių gynimo mechanizmo lygių atžvilgiu. Tačiau, atsižvelgiant į bendros mechanizmo struktūros sudėtingumą ir trūkumą, DG29 nuogaustauja, kad praktiškai ribojamas efektyvus naudojimasis duomenų subjekto teise. DG29 pažymi, kad teisių gynimo mechanizmo kokybei turi būti teikiama pirmenybė ES asmenims siūlomų mechanizmų kiekio atžvilgiu. Taip pat nerimaujama dėl to, kad daugumos, jeigu ne visų, teisių gynimo priemonių atveju numatoma atitinkama procedūra JAV, taip komplikuojant ES DAI stebėsenos procedūrą.

Faktiškai, teisių gynimo mechanizmo, numatyto „privatumo skyde“, atveju dėmesys visų pirma sutelkiamas ties duomenų subjekto galimybe „apginti savo teises ir iškelti bylas dėl privatumo principų nesilaikymo, kreipiantis tiesiogiai į JAV autosertifikuotą bendrovę“²⁷. Be to, organizacijos turi paskirti nepriklausomą ginčų sprendimo įstaigą, kuri nagrinės ir spręs asmenų pateiktus skundus. DG29 palankiai vertina tai, kad tai bus organizuojama nemokamai.

Skundai taip pat gali būti teikiami tiesiogiai Federalinei prekybos komisijai, netgi jeigu FPK neprivalo jų nagrinėti. DAI taip pat gali pateikti skundą, o PD įsipareigojo peržvelgti ir visomis išgalėmis stengtis supaprastinti skundų, kurie Federalinės prekybos komisijos bus nagrinėjami prioritetine tvarka (II priedas, III.7.e skirsnis), sprendimą (I priedas). Tačiau FPK pirmenybės skundams teikimo tvarka duomenų subjektui neužtikrina jokio užtikrintumo, kad jo skundai bus nagrinėjami.

Kraštutiniu atveju asmenys galės kreiptis į privalomą arbitražą. Arbitrų kolegija bus įsikūrusi JAV, o jos sprendimus peržiūrės JAV teismai.

²⁷ Europos Komisija, sprendimo dėl tinkamumo projektas, 30 sk.

„Privatumo skyde“ taip pat numatoma galimybė organizacijai pasirinkti bendradarbiavimą su ES DAI (II priedas, III.5.a skirsnis). Tai net privaloma duomenų apie žmogiškuosius išteklius, renkamų užmezgant darbo santykius, atveju (II priedas, III.9.d.ii skirsnis). Tokiu atveju alternatyvus ginčų nagrinėjimas (AGN) nebus taikomas (II priedas, III.5.a skirsnis). „Privatumo skydo“ nuostatose aiškiai nenurodyta, kaip praktiškai bus organizuojamas bendradarbiavimas su ES DAI. Tiksliau, neaišku, ar kolegija spręs visas bylas, ar kiekviena atskira byla bus nagrinėjama vis kitos kolegijos.

DG29 mano, kad sprendimas dėl tinkamumo turi būti išsamesnis dėl DAI kompetencijos nagrinėti skundus. Atrodo, kad tai priklauso nuo organizacijos kvalifikavimo, tačiau neaišku koku būdu.

Jeigu organizacija ES duomenų valdytojo vardu veikia kaip atstovė, bet koku atveju asmenys gali skųstis kompetentingai ES DAI. Situacija bus panaši tiek žmogiškųjų išteklių, tiek kitų komercinių duomenų tvarkymo atveju.

Jeigu „privatumo skydo“ organizacija veikia kaip duomenų tvarkytoja, DAI kompetencija nagrinėti skundą apsiribos duomenų tvarkymu pagal ES įstatymus (duomenų tvarkymas ES duomenų tvarkytojui prisiimant atsakomybę – įskaitant bendrą valdymą su JAV organizacija – arba jeigu „privatumo skydo“ organizacijai tiesiogiai galioja ES įstatymai, pavyzdžiui, naudojant įrangą ES). Tačiau, kai duomenų tvarkymas vykdomas tik pagal JAV įstatymus, bus išskirtinai taikomi „privatumo skydo“ mechanizmai. Siekiant įveikti JAV teisinės sistemos kalbos barjerą ir žinių trūkumą, gali būti paranku, jeigu ES DAI turėtų teisę veikti kaip tarpininkės, nagrinėjant asmenų skundus, arba padėti vykdyti AGS procedūras kartu su JAV organizacijomis arba kreipiantis į JAV valdžios įstaigas, jeigu DAI mano, kad tai reikalinga.

DG29 pabrėžia, kad „privatumo skyde“ apibūdintas mechanizmas neatitinka anksčiau pateiktos rekomendacijos, remiantis kuria ES asmenys turėtų „galėti teikti reikalavimus dėl žalos atlyginimo Europos Sąjungoje“ ir „turėti teisę teikti reikalavimus kompetentingame ES teisme.“²⁸ Būtų pritarta, jeigu „privatumo skydo“ organizacijos įtrauktų tokią galimybę į savo privatumo politiką.

Siekdama užtikrinti efektyvumą, DG29 rekomenduoja, kad sistema ES DAI sudarytų sąlygas atstovauti duomenų subjektui ir veikti jo vardu arba veikti kaip tarpininkui. Kita vertus, joje turėtų būti numatytos specialios nuostatos dėl jurisdikcijos, duomenų subjektams suteikiančios teisę naudotis savo teisėmis Europoje.

b) Arbitražas

Galutinės arbitražo procedūros dar nebaigtos, dėl to DG29 įvertinimas yra sudėtingas. Kadangi atrodo, jog arbitražo sistema taikoma pagal JAV įstatymus ir kad vienintelė proceso kalba bus anglų kalba, ES DAI gali pageidauti teisės padėti asmenims proceso metu.

²⁸ Žr. DG29 raštą pirmininko pavaduotojai V. Reding, 2014 m. balandžio 10 d.

Be to, arbitražo procedūra nustatyta dėl to, kad nebuvo garantijos, jog skundas bus nagrinėjamas, kadangi FPK neprivalo nagrinėti kiekvieno skundo. Jeigu ES asmuo manys, jog jam reikia advokato pagalbos, DG29 pažymi, kad jis pats turės sumokėti savo advokato mokesčius, o tai asmenims gali būti kliūtis skųstis arbitražui.

c) Teisių gynimo institucijų priežiūra, įgyvendinimas ir veiksmingumas

Prisijungimo prie „skydo“ sąlygos

ESTT teigimu, „autosertifikavimo sistemos patikimumas [...] iš esmės pagrįstas veiksmingų nustatymo ir priežiūros mechanizmu, kurie sudaro sąlygas taisyklių pažeidimams užtikrinant pagrindinių teisių apsaugą, kūrimu [...]“²⁹.

DG29 pažymi, kad PD „privatumo skydo“ vaidmuo sertifikavimo procese sumažinamas iki dokumentų išsamumo tikrinimo. Nors DG29 pripažįsta, kad autosertifikavimas nereiškia sisteminio privatumo politikos įgyvendinimo patikrinimo *a priori*, PD turėtų bent įsipareigoti sistemingai tikrinti, kad privatumo politika atitiktų visus „privatumo skydo“ principus. Toks įsipareigojimas minimas sprendimo dėl tinkamumo projekte, tačiau negali būti aiškiai nustatytas PD pareiškimo rašte³⁰.

„Privatumo skydo“ principų pažeidimas gali būti nepastebėtas ilgą laiko tarpą ir gali būti nustatytas tik rimtai pažeidus pagrindines duomenų subjekto teises, galbūt be atkūrimo galimybių. Taigi, šis požiūris gali prieštarauti Europos atsargumo principui.

Skaidrumo užtikrinimas, taikant „privatumo skydo“ sąrašo ir iš sąrašo pašalintų organizacijų registravimo priemones

Skaidrumas duomenų subjekto atžvilgiu buvo žymiai pagerintas. Be visų JAV organizacijų, kurios pateikė PD autosertifikavimo pažymėjimą, naujajame „privatumo skydo“ sąrašo sąrašo taip pat bus pateiktas visų iš „privatumo skydo“ sąrašo išbrauktų organizacijų registras, įskaitant priežastį, kodėl organizacija buvo išbraukta.³¹ PD „privatumo skydo“ svetainė bus geriau pritaikyta tikslinėms auditorijoms, supaprastinant organizacijos autosertifikavimo pažymėjime pateiktos informacijos tipo bei privatumo politikos, kuri taikoma susijusiai informacijai, bei metodo, kurį organizacija taiko principų laikymosi patikrinimams, patikrinimą.³² DG29 palankiai vertina faktą, kad dabar yra aišku, jog PD patikrins, ar bendrovės, kurios turi viešuosius tinklalapius, juose paskelbė savo privatumo politiką arba,

²⁹ ESTT, *Schrems*, 81 sk.

³⁰ Europos Komisija, sprendimo dėl tinkamumo projektas, 34 sk.

³¹ I priedo 5 p. ir II priede, II.1 skirsnyje DG29 taip pat mini ketvirtąją Komisijos rekomendaciją, pateiktą Komunikate COM(2103)847 bei 2014 m. balandžio 10 d. DG29 rašte pirmininko pavaduotojai V. Reding, tiksliau, skyriaus „Skaidrumas“ 5 punktą.

³² I priedo 8 p. DG29 taip pat mini savo 2014 m. balandžio 10 d. raštą pirmininko pavaduotojai V. Reding, tiksliau, skyriaus „Skaidrumas“ 2 punktą.

jeigu jos viešųjų tinklalapių neturi, kur privatumo politika skelbiama³³. Dokumentuose taip pat pateikiama daugiau informacijos apie privatumo politikos turinį³⁴.

DG29 mano, kad problemų gali kilti, jeigu organizacija, kuri jau įtraukta į „privatumo skydo“ sąrašą, vėliau sertifikavimą išplečia, pridėdama kitas duomenų kategorijas. Tokiais atvejais sąrašas neatspindės įvairių principų taikymo įvairioms duomenų kategorijoms laikotarpių. Tokiu būdu kyla rizika, kad ES asmenys ir verslo atstovai negalės atlikti viso įvertinimo, ar „privatumo skydo“ principai taikomi specialioms duomenims, o jeigu taip, nuo kada. Siekiant išvengti šio trūkumo, darbo grupė rekomenduoja, kad „privatumo skydo“ sąraše pateiktame organizacijų registre kiekvienai asmeninių duomenų kategorijai būtų atskirai nurodyti duomenys apie autosertifikavimo įsigaliojimą.

DG29 palankiai vertina tai, kad PD ves organizacijų, kurios buvo ištrintos iš „privatumo skydo“ sąrašo, registrą ir kad į tą registrą bus įtrauktas paaiškinimas, kad tos organizacijos nebegali naudotis „privatumo skydo“ privilegijomis, tačiau turi ir toliau vadovautis principais, galiojančiais asmens duomenims, kurie buvo gauti tai organizacijai būnant sertifikuota „privatumo skydo“ organizacija, tol, kol ji tokius duomenis saugo (I priedas, 3 p.). Tačiau, kadangi kai kurios organizacijos, kurios buvo išbrauktos iš „privatumo skydo“ sąrašo, gali nuspręsti grąžinti ar ištrinti pagal „privatumo skydo“ nuostatas gautus duomenis, o kitos organizacijos saugos duomenis, kuriuos jos gavo pagal „skydo“ nuostatas, svarbu asmenims užtikrinti didesnę skaidrumą šiuo klausimu. Todėl PD prižiūriname bendrovių registre turi būti nurodyta, ar organizacija vis dar saugo asmens duomenis, gautus pagal „privatumo skydo“ nuostatas, arba ar ji grąžino ar ištrinė tokius duomenis. Jeigu organizacija vis dar saugo tokius duomenis, registre turi būti aiškiai nurodyta, kad organizacija tokiems duomenims turi ir toliau taikyti Principus.

Be to, PD vedamame registre turi būti nurodyta, kad tos organizacijos daugiau nebegali naudotis „privatumo skydo“ privilegijomis naujiems duomenų perdavimams, o tai reiškia, kad organizacijai nebeleidžiama gauti asmens duomenų iš ES vadovaujantis Principais.

³³ I priede, 3 ir 4 punkte DG29 taip pat mini pirmąją Komisijos rekomendaciją, pateiktą Komunikate COM(2103)847 bei 2014 m. balandžio 10 d. DG 29 rašte pirmininko pavaduotojai V. Reding, tiksliau, skyriaus „Skaidrumas“ 3 punktą.

³⁴ I priedas, 5 ir 6 p. bei II priedas, III.6 skirsnis.

Patikros procedūros

Siekdamos patikrinti, ar autosertifikavimas yra veiksmingas praktikoje, organizacijos gali atlikti savęs vertinimą arba pasitelkti atitikties peržiūras iš išorės. DG29 apgailestauja, kad darbuotojų mokymai yra reikalingi tik kai organizacija nusprendžia atlikti patikrinimą vykdydama autosertifikavimą (II priedas, III.7.c skirsnis). Taip pat atrodo, kad poreikis patikrinti, kad taisyklės yra teisingos, visapūsės, aiškiai išdėstytos, visiškai vykdomos ir prieinamos, yra neišvengiamas tik jeigu organizacija pasirenka atlikti vidinį patikrinimą (savęs vertinimą) ir toks patikrinimas, pasitelkiant išorinį mechanizmą, apsiriboja organizacijos privatumo politikos taisyklių laikymusi.

A posteriori

DG29 palankiai vertina tai, kad FPK ir PD suteikti tyrimo įgaliojimai skundų atveju. Be to, DG29 pažymi, kad PD turės galimybę atlikti *ex officio* patikrinimus, visų pirma siųsdamas klausimynus. Tačiau DG29 norėtų įsitikinti, kad tokio požiūrio pakanka norint įgyvendinti ESTT veiksmingo pažeidimo nustatymo ir priežiūros mechanizmų reikalavimą. Faktiškai DG29 vis dar turi klausimų dėl tikslų JAV teisėsaugos institucijų įgaliojimų vykdyti patikrinimus vietoje autosertifikuotų organizacijų patalpose, siekiant išnagrinėti „privatumo skydo“ nuostatų pažeidimus, kaip gali būti taikoma ES įstaigos sprendimo *egzekvatūra* JAV teritorijoje ir ar pagal „privatumo skydo“ nuostatas taikomos sankcijos praktikoje yra atgrasančios.

2.2.7 Žmogiškųjų išteklių duomenų tvarkymas

Taikymo sritis

9 papildomas principas (II priedas, III.9 skirsnis) taikomas asmeninei informacijai apie darbuotoją (buvusį ar esamą), kuri buvo surinkta dėl darbo santykių. Remiantis 9 papildomo principo a.ii punkto formuluote, „privatumo skydo“ principai taikomi, tik kai „perduodami ar prieinami asmenį identifikuojantys įrašai“. Terminas „identifikuojantys įrašai“ prieštarauja „asmeninių duomenų“ apibrėžimui pagal II priedą, I.8.a skirsnį, kuris taikomas „duomenims apie identifikuatą arba identifikuojamą asmenį“ ir todėl nedera su direktyvoje naudojama apibrėžtimi³⁵.

9 papildomo principo a.ii punkte nurodyta, kad „Statistiniai pranešimai, sudaryti remiantis bendrais įdarbinimo duomenimis, kuriuose nepateikti asmeniniai duomenys ir kuriems nenaudojami anoniminiai duomenys, su privatumu nesietini“. Šis teiginys prieštarauja įvairioms nuomonėms, pateiktoms DG29. DG29 norėtų pabrėžti, kad suvestiniai duomenys gali būti pakartotinai identifikuoti ir todėl turėtų būti laikomi asmeniniais duomenimis³⁶.

³⁵ Kaip pabrėžta anksčiau, apsiribojimas duomenimis, kurie „perduodami ar prieinami“, taip pat nedera su terminu „tvarkymas“ (II priedas, I.8.b skirsnis).

³⁶ Žr. Nuomonę 4/2007 dėl asmeninių duomenų koncepcijos bei Nuomonę 05/2014 dėl nuasmeninimo technikos.

Pranešimas, pasirinkimas ir tikslo ribojimas

9 papildomo principo b.i punkte pateiktas Pranešimo ir Pasirinkimo principų taikymo pavyzdys, kai duomenys apie žmogiškuosius išteklius naudojami kitais tikslais. Šis pavyzdys yra JAV organizacija, kuri „ketina panaudoti darbo santykių metu surinktą asmeninę informaciją su darbo santykiais nesusijusiais tikslais, pvz., rinkodaros pranešimuose“. Šiame scenarijuje tikslas gali būti pakeistas, su sąlyga, kad laikomasi Pranešimo ir Pasirinkimo principo. DG29 nuomone, tolesnis duomenų apie žmogiškuosius išteklius tvarkymas tiesioginės rinkodaros tikslais daugeliu atvejų bus laikomas nesuderinamu tikslu ir todėl prieštaraujantis Tikslo ribojimo principui (II priedas, II.5.a skirsnis). Be to, DG29 mano, kad pasirinkimas negali būti tinkamas pagrindas darbuotojui „sutikti“ (pasirinkti), kad tikslas būtų pakeistas, kai darbo santykiuose toks sutikimas gali būti nevisiškai laisvas.

DG29 labai abejoja, ar „privatumo skydo“ nuostatose skiriamas didžiausias dėmesys Pasirinkimo principui, kaip tolesnio duomenų naudojimo kitais tikslais sąlygai, atitinka EBPO privatumo direktyvas, kadangi nėra pakankamai garantijų, būtinų siekiant užkirsti kelią, kad šis pasirinkimo mechanizmas taip pat galėtų būti naudojamas tolesniam duomenų tvarkymui, jeigu jis yra nesuderinamas. 9 papildomo principo b.iv punkte nurodyta plati ir aiški Pranešimo ir Pasirinkimo principų išimtis „laikotarpiui, būtinam, kad nebūtų pakenkta organizacijos gebėjimams, kai paaukštinama pareigose, skiriama į pareigas ar priimami kiti panašūs darbo santykių sprendimai“. Pirma, žmogiškųjų išteklių duomenų naudojimas tokiais tikslais turi būti aiškiai nurodytas renkant duomenis. Be to, formuluotė „kiti panašūs darbo santykių sprendimai“ yra per daug netiksli ir per plati. Dėl to žmogiškųjų išteklių duomenims nebus taikomas Pranešimo ir Pasirinkimo principas, kai duomenys tvarkomi darbo santykių kontekste. Šis terminas yra per platus, jis nesudaro sąlygų įvertinti, ar tolesnis naudojimas yra suderinamas su pradiniu tikslu. DG29 rekomenduoja pašalinti šią išimtį.

Prieigos teisė

9 papildomo principo e.i punkte taip pat nurodyta Prieigos principo taikymo arba trečiosios šalies duomenų valdytojo sutarties sudarymo išimtis, kai tai susiję su nereguliaria su darbo santykiais susijusia veikla – pavyzdžiui, skrydžio, viešbučio kambario užsakymu arba draudimu – nedidelio darbuotojų skaičiaus asmens duomenys gali būti perduodami ir pateikiami, jeigu laikomasi Pranešimo ir Pasirinkimo principo. DG29 nemato pagrįsto tokios išimties pateisinimo ir rekomenduoja pašalinti šį punktą.

2.2.8 Farmaciniai ir medicinos produktai

Taikymo sritis

Remiantis „privatumo skydo“ nuostatomis, raktu užkoduotų duomenų perdavimai iš Europos Sąjungos į JAV farmacinių ir medicinos produktų atveju nereiškia perdavimo, kuriam taikomos „privatumo skydo“ nuostatos (II priedas, III.14.g.i skirsnis). Tačiau raktu užkoduotų duomenų perdavimas apsaugomas pagal Europos duomenų apsaugos įstatymus. Tai reiškia, kad praktiškai „privatumo skydas“ negalioja tokiems perdavimams. DG29 ragina ES

Komisiją aiškiai nurodyti, kad sprendimo dėl tinkamumo projektas neapima raktu užkoduotų duomenų perdavimo dėl farmacinių ir medicininių priemonių ir dėl to tokiems perdavimams turi būti taikomos kitos apsaugos priemonės, pavyzdžiui, standartinės sutarčių sąlygos (toliau: SSS) arba privalomos įmonių taisyklės. DG29 siūlo tai paaiškinti galutiniam sprendime dėl tinkamumo.

Perdavimai priežiūros ir kontrolės tikslais (II priedas, III.14.d skirsnis)

DG29 nuogąstauja, kad pagal šias nuostatas asmeniniai duomenys, kurie dėl medicininio pobūdžio dažniausiai yra slapti, gali būti perduoti reguliavimo institucijoms JAV. Kadangi „privatumo skydas“ skirtas duomenų perdavimui tarp privačių subjektų, panašu, kad viešoji įstaiga, pvz., JAV reguliavimo institucija, neturi teisės autosertifikuotis pagal „privatumo skydo“ nuostatas, dėl ko kyla atitinkamas duomenų apsaugos klausimas tokių perdavimų atveju. Jeigu tokie perdavimai turi būti administruojami kontrolės tikslais, turi būti imtasi atitinkamų priemonių, siekiant užtikrinti pagrindinių ES duomenų subjekto teisių apsaugą. DG29 pabrėžia, kad sprendimo dėl tinkamumo projekte nepateikiama išvadų šiuo klausimu. Todėl DG29 neturi jokių garantijų, kad ES duomenų subjektų slapti duomenys bus atitinkamai apsaugoti šiuo atžvilgiu.

Be to, DG29 pažymi, kad nesupranta, kodėl „rinkodaros“ tikslas nurodomas kaip duomenų tvarkymo būsimam moksliniam tyrimui pavyzdys. Be to, tolesnio perdavimo į bendrovės buveinę ir kitiems tyrėjams priežastis (II priedas, III.14.d skirsnis), nurodyta skyriuje „Perdavimai priežiūros ir kontrolės tikslais“, yra neaiški. Šiuos klausimus būtina paaiškinti galutiniam sprendime dėl tinkamumo.

Produktų saugumas, veiksmingumo stebėseną (įskaitant ataskaitas valdžios įstaigoms) ir pacientų, vartojančių tam tikrus medikamentus ar naudojančių tam tikrus medicinos įtaisus, sekimas

„Privatumo skydo“ nuostatose pateikiama Pranešimo, Pasirinkimo, Tolesnio perdavimo ir Prieigos principų išimtis tiek, kiek Principų laikymasis kliudo norminių reikalavimų vykdymui. Sprendimo dėl tinkamumo projekte nenurodomos išvados dėl situacijos, kai Privatumo principai kliudo norminių reikalavimų vykdymui. Jeigu DG29 supranta, kad vyriausybės tyrimai gali pateisinti pranešimo ir prieigos teisės apribojimus, siekiant apsaugoti tyrimus, DG29 nemato priežasčių, dėl kurių galima pateisinti tokias plačias išimtis, kai duomenys tvarkomi privačiam sektoriui priklausančios organizacijos ar trečiosios šalies. Pavyzdžiui, kadangi pacientai gydomi vis labiau individualizuotai, tokia plati Privatumo principo išimtis pacientų, vartojančių tam tikrus medikamentus ar naudojančių tam tikrus medicininius įtaisus, sekimo atveju yra nepriimtina, kadangi tokio tipo priežiūra bus dažna. Tai taip pat galioja, kai duomenys naudojami farmacijos bendrovių produktų saugumo, veiksmingumo stebėjimo tikslais (naujų medikamentų bandymas ar prekyba jais).

2.2.9 Viešai prieinama informacija

Prieigos teisės išimtis viešai prieinamos ir viešųjų archyvų informacijos atveju (II priedas, III.15.d ir e skirsnis) kelia abejonių dėl to, kad kai asmuo naudoja savo prieigos teisėmis, jis pageidauja žinoti, ar tam tikras duomenų tvarkytojas tvarko duomenis apie jį, ir kokie duomenys tvarkomi, siekdamas kontroliuoti jo duomenų tvarkymą. DG29 ne kartą pareiškė, kad pagal ES įstatymus duomenų subjektai visada turi teisę į prieigą prie savo duomenų ir, jeigu reikia, paprašyti, kad jie būtų ištaisyti ar pašalinti, jeigu jie nebuvo tvarkomi teisėtai arba jeigu jie yra nesuderinami ar netikslūs, nepaisant to, ar asmens duomenys buvo skelbiami.³⁷ Jeigu asmens prašymas leisti susipažinti su duomenimis atmetamas dėl to, kad duomenys buvo gauti iš viešai prieinamų šaltinių ar viešųjų registų, asmuo netektų galimybes kontroliuoti duomenų tikslumą ir tikrinti, ar iš pradžių duomenys buvo pavišinti teisėtai.

Tačiau pagal „privatumo skydo“ nuostatas viešiesiems registrams ir viešai paskelbtai informacijai netaikomi Pranešimo, Pasirinkimo, Prieigos ir Atskaitomybės už tolesnį perdavimą principai (II priedas, II.15.b skirsnis). Šios išimties atrodo per plačios, palyginti su direktyva, ir kelia susirūpinimą, kadangi, be kita ko, jos mažina asmenų galimybes kontroliuoti duomenų tikslumą ir riboti jų duomenų platinimą.

2.3 Išvados

DG29 pripažįsta, kad JAV valdžios įstaigos ir Europos komisija labai pagerino komercinius duomenų perdavimo tarp dviejų kontinentų aspektus. Tačiau atsižvelgdama į pirmiau pateiktą analizę, DG29 mano, kad „privatumo skydo“ komercinę pusę reikia išsamiau paaiškinti įvairiais atžvilgiais. Pavyzdžiui, aiškaus duomenų saugojimo principo trūkumas kelia susirūpinimą. Todėl DG29 yra rimtai susirūpinusi dėl to, ar „privatumo skydas“ gali užtikrinti apsaugos lygį, kuris iš esmės atitinka ES užtikrinamą lygį.

Sprendime dėl tinkamumo reikia išsamiau paaiškinti Tikslų ribojimo ir Pasirinkimo principus. Išlieka spragų rizika kelių principų atžvilgiu, ypač tolesnio perdavimo, skundų nagrinėjimo institucijų ir žmoniškųjų išteklių ar farmacinių duomenų tvarkymo. Be to, reikia patobulinti tvarką, kaip „privatumo skydo“ principai taikomi duomenų tvarkytojams (atstovams), ir būtina skirti dėmesio aiškaus ir tiksliai apibrėžto terminologijos taikymo užtikrinimui.

3. SPRENDIMO DĖL TINKAMUMO PROJEKTO NACIONALINIO SAUGUMO GARANTIJŲ ĮVERTINIMAS

3.1 JAV nacionalinio saugumo įstaigoms taikomos apsaugos priemonės ir apribojimai

Pagrindinių teisių į privatą gyvenimą ir duomenų apsaugą pažeidimas leidžiamas, tik jeigu toks pažeidimas pateisinamas demokratinėje visuomenėje. Tai reiškia, kad Privatumo principai nėra absoliutūs ir kad galimi nukrypimai, bet tik jeigu užtikrinamos taikomos (esminės) garantijos. Siekdamas privatumo apsaugos stiprinimo, organizacijos turi stengtis visiškai ir skaidriai įgyvendinti Principus, o jei JAV teisės aktuose leidžiamos Principų

³⁷ Žr. WP20, 4 p.

išimty bus taikomos reguliariai, jos turi tai nurodyti savo privatumo taisyklėse. Dėl tos pačios priežasties pageidaujama, kad tais atvejais, kai pagal Principus ir (arba) JAV teisės aktus galima pasirinkti kelis variantus, organizacijos pasirinktų geriausią apsaugą suteikiantį variantą.

II priede, I.5 skirsnyje nurodyta, kad „Privatumo principų laikymasis gali būti ribojamas: (a) tiek, kiek būtina, atsižvelgiant į nacionalinio saugumo, visuomenės interesų ar teisės aktų laikymosi reikalavimus; (b) įstatymais, Vyriausybės nutarimais arba teismų praktika, dėl kurių atsiranda prieštarų išipareigojimų ar aiškių įgaliojimų, jeigu vykdydama tokius įgaliojimus organizacija gali įrodyti, kad Principų nesilaikoma tik tiek, kiek tai būtina atsižvelgiant į organizacijos palaikomus viršesnius teisėtus interesus; arba c) jei valstybės narės įstatymai dėl Direktyvos numato išimtis ar leidžiančios nukrypti nuostatos taikomos dėl panašių priežasčių.

Tik klausimas, ar II priede minėtos leidžiančios nukrypti nuostatos pateisinamos demokratinėje visuomenėje. Kaip nurodyta „privatumo skydo“ sprendimo dėl tinkamumo projekte, Komisija mano, kad „Jungtinėse Amerikos Valstijose galioja taisyklės, kuriomis ribojamas bet koks kišimasis į asmenų, kurių asmens duomenys perduodami iš Sąjungos į Jungtines Amerikos Valstijas pagal „privatumo skydą“, pagrindines teises nacionalinio saugumo tikslais tiek, kiek tai griežtai būtina siekiant atitinkamo teisėto tikslo“³⁸.

Taikydamą sistemą, nurodytą šios nuomonės 1.2 skyriuje ir atsižvelgdama į JAV valdžios įstaigų pareiškimus ir Komisijos išvadas, DG29 įvertino esamą JAV teisinę sistemą ir JAV žvalgybos agentūrų praktiką ir sąlygas, pagal kurias leidžiamas kišimasis į pagrindines teises į privatų gyvenimą ir duomenų apsaugą, užtikrinamą remiantis Europos teisės aktais. Šis įvertinimas pagrįstas Prezidento politinės direktyvos Nr. 28 (PPD-28), Vykdomojo įsako 12333 (EO12333) analize ir įvairiais teisiniais pagrindais, numatytais Užsienio žvalgybos akte (FISA – 104 skyrius, 402 skyrius, 215 skyrius, 501 skyrius ir 702 skyrius). DG29 rėmėsi „privatumo skydo“ VI priedu, kuris sudarytas iš Nacionalinės žvalgybos direktoriaus biuro (ODNI) paruošto rašto dėl JAV nacionalinio saugumo įstaigoms taikomų apsaugos priemonių ir apribojimų ir informacijos apie JAV signalų žvalgybos veiklą, kuri buvo pateikta Europos Komisijai.

3.2 A garantija: duomenų tvarkymas turi atitikti įstatymus ir būti paremtas aiškiomis, tiksliais ir prieinamomis taisyklėmis

Remiantis Europos teisės aktais, kišimasis turi atitikti įstatymus, nustatytas taisykles ir procedūras bei turi būti pakankamai aiškus ir prieinamas (atsižvelgiant į konkrečiose šalyse galiojančius apribojimus), siekiant piliečiams suteikti atitinkamą informaciją apie aplinkybes, kurioms esant valdžios institucijoms suteikiami įgaliojimai imtis žvalgybos priemonių.³⁹

³⁸ Komisijos sprendimo projektas, remiantis Europos Parlamento ir Tarybos direktyva 95/46/EB dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo, 75 sk.

³⁹ EŽTT *Zakharov* 247 sk. „Teismas anksčiau nusprendė, kad įstatymuose reglamentuotas „numatomumo“ reikalavimas netaikomas tiek, kad valstybės būtų priverstos paskelbti teisinės nuostatas, kuriose išsamiai išvardinti veiksmai, kurie gali paskatinti sprendimą asmeniui taikyti slapto sekimo priemones „nacionalinio saugumo“ pagrindais. Atsižvelgiant į pobūdį,

DG29 pažymi, kad signalų žvalgybos veikla vykdoma prieinamos teisinės sistemos pagrindu. Visi VI priede minėti įstatymai (PPD-28, FISA, USA FREEDOM ACT, FOIA) skelbiami internete (JAV ir už jų ribų). VI priede pateikiama galiojančių teisės nuostatų santrauka, duomenų rinkimo, saugojimo ir skleidimo apribojimai, atitikties ir priežiūros, skaidrumo bei žalos atlyginimo nuostatos. JAV žvalgybos veiklos teisės aktai sudaryti iš įvairių dokumentų, įskaitant agentūrų ataskaitas, taisykles ir procedūras, kurios turi būti analizuojamos, siekiant geresnio supratimo apie tai, kaip vykdoma veikla, tiek teoriškai, tiek praktiškai. Šiuo atžvilgiu DG29 dėmesį sutelkė ties ribotu, jos nuomone, svarbiausių klausimų skaičiumi.

3.2.1 Vykdomasis įsakas Nr. 12333 ir Prezidento politinė direktyva Nr. 28

EO12333 taikymo sritis yra plati; iš esmės užsienio žvalgybos duomenų rinkimas, remiantis Įsaku, gali būti vykdomas JAV prezidento nuožiūra. Tačiau buvo tvirtinama, kad nuo FISA paskelbimo EO12333 gali būti naudojamas tik duomenų rinkimui už JAV teritorijos ribų. DG29 pažymi, kad EO12333 nepateikiama labai išsami informacija apie geografinį regioną, duomenų rinkimo, saugojimo ar tolesnio skleidimo apimtis bei apie nusikaltimų, dėl kurių gali būti imtasi žvalgybos priemonių, arba informacijos, kuri gali būti renkama ar naudojama, pobūdį.

DG29 supratimu, pagrindinis Prezidento politinės direktyvos Nr. 28 (PPD-28) tikslas yra nustatyti asmens duomenų rinkimo ir tvarkymo ribas, nepriklausomai nuo to, kokia žvalgybos programa taikoma ir kur buvo gauti duomenys.

PPD-28 yra Jungtinių Amerikos Valstijų prezidento direktyva, kurioje apibrėžti nuoseklumo principai, kuriais remiantis leidžiama vykdyti signalų žvalgybos veiklą ir ji yra vykdoma, tačiau PPD-28 nėra teisinis duomenų rinkimo pagrindas. PPD-28 yra veiksminga, kai tie principai taikomi žvalgybos bendruomenės institucijoms, kad šios įgyvendintų juos vykdydamos savo politiką ir procedūras. Direktyva galioja signalų žvalgybos veiklai, nepriklausomai nuo duomenų vietos duomenų rinkimo metu JAV ar už jų ribų. Todėl ji taip pat galioja duomenims, kurie renkami signalų žvalgybos tikslais, kai jie perduodami iš ES į Jungtines Amerikos Valstijas.

Tiksliau, PPD-28 nurodoma, kad signalų žvalgybos veikla turi būti kuo geriau pritaikyta⁴⁰. Duomenų naudojimo atžvilgiu numatomos duomenų kiekio mažinimo (įskaitant duomenų saugojimo ir skleidimo sąlygas), duomenų saugumo ir prieigos personalui [t. y. taisyklės, kuriose numatomos apsaugos priemonės, ribojančios piktnaudžiavimo ir netinkamo naudojimo riziką], duomenų kokybės užtikrinimo ir priežiūros procedūros. Šios garantijos taikomos nepriklausomai nuo duomenų subjektų tautybės, t. y. JAV ir ne JAV asmenims.

grėsmės nacionaliniam saugumui gali skirtis ir gali būti neįmanoma jų numatyti arba gali būti sudėtinga jas iš anksto nustatyti (žr. Kennedy, kaip minėta pirmiau, 159 sk.). Tuo pat metu teismas taip pat pabrėžė, kad pagrindinėms teisėms įtakos turinčiais atvejais tai prieštarautų galiojantiems įstatymams, vienam pagrindinių Konvencijoje numatytų demokratinės visuomenės principų, atsižvelgiant į nacionalinio saugumo vykdomajai institucijai suteiktas laisves, išreikštas nevaržomos galios forma. Todėl įstatymuose turi būti aiškiai numatytos tokių kompetentingoms įstaigoms suteiktų laisvių apimtys ir naudojimosi jomis būdai, atsižvelgiant į atitinkamos priemonės teisėtą tikslą, siekiant asmeniui užtikrinti atitinkamą apsaugą nuo savavališko kišimosi“.

⁴⁰ „Signalų žvalgybos veikla turi būti kuo tikslingesnė. Nustatydamos, ar verta rinkti signalų žvalgybos duomenis, Jungtinės Amerikos Valstijos privalo išnagrinėti kitos informacijos prieinamumą, įskaitant diplomatinį ir viešų šaltinių. Reikėtų teikti pirmenybę tokioms tinkamoms ir įgyvendinamoms signalų žvalgybos alternatyvoms“ (1 skyriaus d dalis).

Perduodant duomenis į JAV, taip pat taikytinos PPD-28 nustatytos apsaugos priemonės. VI priede pateiktas ODNI įsipareigojimas, kad jeigu JAV žvalgybos bendruomenė turi rinkti duomenis iš transatlantinių kabelių, juos perduodant į Jungtines Amerikos Valstijas, „ji tai darytų taikydama šiame rašte nustatytą apribojimų ir apsaugos priemonių, įskaitant PPD-28, reikalavimus“⁴¹. DG29 pažymi, kad vis dar nėra nusistovėjusios teismų praktikos, apsprendžiančios bet kurios šalies atliekamo kabelių perėmimo teisėtumą. Bet kokių atveju JAV nei patvirtina, nei paneigia, kad jos naudoja kabelių perėmimą kaip žvalgybos duomenų rinkimo priemonę.

„Signalų žvalgybos“ sąvoka neapibrėžta nei PPD-28, nei jokiame kitame tekste.

3.2.2 Užsienio žvalgybos stebėjimo aktas

Apskritai FISA tekstas atrodo aiškesnis ir tikslesnis. Tačiau daugelio nuostatų aiškinimas PPD-28 kontekste ir jų praktinis taikymas labai priklauso nuo įvairių agentūrų įgyvendinimo. Kadangi kol kas nepateikta išsami naujų apsaugos priemonių įgyvendinimo ataskaita, JAV delegatai informavo DG29 atstovus, kad PPD-28 saugumo priemonių įgyvendinimas iš tikrųjų baigtas ir visoje JAV žvalgybos bendruomenėje atliekamas panašiai.

Tiksliau, 501 skyrius yra santykinai aiškus žvalgybos operacijų, kurioms gali būti suteiktas leidimas, tipo atžvilgiu: „materialių daiktų gamyba (įskaitant knygas, įrašus, raštus, dokumentus ir kt.)“. Tačiau reikėtų paminėti, kad dėl to, jog terminas „materialūs daiktai“ apima ir „kt.“, šių įgaliojimų apimtys yra gana plačios.

702 skyriuje, kuriuo remiantis duomenis leidžiama rinkti iš ne JAV asmenų, kurie, tikėtina, yra už Jungtinių Amerikos Valstijų ribų, siekiant gauti užsienio žvalgybos informaciją,⁴² nepateikiami tokie išsamūs duomenys kaip 501 skyriuje. Taikymo srities atžvilgiu, 702 skyrius yra skirtas JAV įsikūrusiems elektroninių ryšių paslaugų teikėjams, kurie renka užsienio žvalgybos informaciją apie už JAV ribų gyvenančius asmenis. „Užsienio žvalgybos informacijos“ apibrėžtis yra plati. Be kita ko, ji apima „informaciją apie užsienio jėgas ar užsienio teritoriją, kuri yra susijusi su Jungtinių Amerikos Valstijų užsienio reikalų tvarkymu“⁴³ o tai kelia neaiškumų dėl informacijos, kuri gali būti renkama praktiškai, tipo.

Nepaisant dokumentų, ataskaitų Kongresui ir Privatumo ir pilietinių laisvių priežiūros valdybos (toliau – PCLOB) priežiūros ataskaitų išslaptinimo, FISA taikymas, įskaitant nurodytą atrankos sąlygų apimtį ir naudojimą, išlieka neaiškus ir painus. Nurodytų atrankos sąlygų („sekami įrenginiai“) naudojimas minimas PCLOB ataskaitoje⁴⁴, tačiau, DG29 nuomone, tai neatitinka sekamų asmenų nustatymo taisyklių, remiantis 702 skyriumi⁴⁵. Kiek DG29 pavyko įsitikinti, bendrai prieinamose taisyklėse jos nenurodomos.

⁴¹ „Privatumo skydas“, VI priedas, Nacionalinės žvalgybos direktoriaus biuro (ODNI) raštas dėl apsaugos priemonių ir apribojimų, taikomų JAV nacionalinio saugumo įstaigoms, 2 p.

⁴² JAV kodekso 50 skyriaus 1 881a (D)(1) skirsnis.

⁴³ JAV kodekso 50 skyriaus 1 801 (e) (2) skirsnis.

⁴⁴ PCLOB ataskaita apie stebėjimo programą, vykdytą pagal FISA 702 skyrių, 32 p.

⁴⁵ JAV kodekso 50 skyriaus 1 881a(D) skirsnis.

3.2.3 Išvada

Apskritai DG29 pažymi, kad taikytini tekstai apie žvalgybos veiklą pateikti internete ir kad JAV valdžios įstaigos ėmėsi įvairių svarbių veiksmų, siekdamos užtikrinti skaidrumą.

DG29 pripažįsta, kad nuo 2013 m. buvo paskelbta daug dokumentų, pavyzdžiui, taisyklės, procedūros, FISC sprendimai ir kiti išslaptinti dokumentai. Be to, PCLOB paskelbė svarbias ataskaitas apie veiklą, vykdomą 702 skyriaus ir JAV laisvės akto pagrindu. Tikimasi, kad panaši ataskaita bus teikiama apie veiklą pagal EO12333.

Keli įstatyminiai priedai, kuriuose gali būti pateikta papildomos informacijos apie vykdomojo įsakymo dėl už Jungtinių Amerikos Valstijų ribų gyvenančių asmenų poveikį, ir taikomos saugumo priemonės yra išslaptinti ir neprieinami visuomenei ar asmenims, kurie nukenčia nuo jų taikymo. Išslaptinti tekstai yra ribotos vertės žvalgybos veiklos atžvilgiu.

Nepaisant pastangų, kurios buvo įdėtos siekiant paaiškinti EO12333 veikimą pagal Snowdeno pateiktą informaciją, ypač patvirtinus PPD-28, dabartinis praktinis EO12333 taikymas lieka neaiškus. DG29 pažymi, kad „privatumo skydo“ VI priede nepateikiama išsami informacija apie EO12333 funkcionavimą.

Nors DG29 palankiai vertina PPD-28 nurodytus apribojimus, sudėtinga išnagrinėti, ar JAV teisinė priežiūros sistema yra pakankamai numatoma, t. y. joje pateikiamos atitinkamos nuorodos apie aplinkybes, kurioms esant valdžios institucijoms suteikiamos galios griebtis tokių priemonių“, kadangi laukiama tolesnio aiškinimo, įskaitant PCLOB ataskaitos paskelbimą pagal EO12333.

3.3 B garantija: turi būti įrodytas būtinumas ir proporcingumas, atsižvelgiant į siekiamus teisėtus tikslus

3.3.1 Prezidento politinė direktyva Nr. 28

Pagal PPD-28 buvo įvesti apribojimai, taikomi tikslams, kuriais gali būti naudojami asmeniniai duomenys, ir sąlygoms, kuriomis jie gali būti skleidžiami bei kurios lemia signalų žvalgybos duomenų rinkimą, nepriklausomai nuo taikomo teisinio pagrindo.

Tiksliau, PPD-28 1 skyriuje tvirtinama, kad JAV signalų žvalgybos veikla visada turi būti kuo tikslingesnė. Pripažįstant šį apribojimą, sudėtinga nustatyti, ar „kuo tikslingesnė“ reiškia, kad visų duomenų rinkimas yra būtinas ir proporcingas.

PPD-28 pripažįsta, kad ir toliau leidžiama vykdyti masinį duomenų rinkimą, „siekiant nustatyti naują ar kylančią grėsmę ir kitą svarbią nacionalinio saugumo informaciją, kuri dažnai paslėpta didelėje ir sudėtingoje modernių pasaulinių komunikacijų sistemoje“.⁴⁶ DG29 pažymi, kad PPD-28 tvirtinama, jog „masiškai surinkti signalų žvalgybos duomenys reiškia didelių signalų žvalgybos duomenų, kurie dėl techninių ar eksploatacinių priežasčių gaunami

⁴⁶ PPD-28, 2 skyrius ir „privatumo skydas“, VI priedas, Nacionalinės žvalgybos direktoriaus biuro (ODNI) raštas dėl saugumo priemonių ir apribojimų, taikomų JAV nacionalinio saugumo įstaigoms, 3 p.

nenaudojant diskriminantų (pvz., konkrečių identifikatorių, atrankos sąlygų, kt.), kiekių rinkimą, kuriam suteiktas leidimas“.

PPD-28 nustatyti masiškai renkamos signalų žvalgybos informacijos naudojimo apribojimai, atsižvelgiant į naudojimo tikslą. Yra šeši tikslai, kuriais informacija gali būti renkama „masiškai“, įskaitant kovą su terorizmu ir kitomis sunkių (tarptautinių) nusikaltimų formomis. DG29 analizėje nurodyta, kad tikslo apribojimas yra gana platus (ir galbūt per platus), kad būtų laikomas tiksliniu.

PPD-28 nepašalina galimybės plačiu mastu masiškai rinkti asmeninius duomenis, o tokio duomenų rinkimo galimybių mastai lieka neaiškūs ir potencialiai platūs. Šiuo atžvilgiu DG29 pažymi, kad VI priede ODNI tvirtina, jog „masinio duomenų rinkimo veikla dėl interneto ryšio, kurią vykdo JAV žvalgybos bendruomenė per signalų žvalgybą, vykdoma mažoje interneto dalyje⁴⁷ ir todėl būtų dėkinga už daugiau įrodymų, pateikiamų naudojantis skaidrumo užtikrinimo priemonėmis.

3.3.2 Užsienio žvalgybos stebėjimo aktas

FISA 215 ir 702 skyriaus minimalios informacijos procedūros buvo nustatytos siekiant JAV asmenis apsaugoti nuo toli siekiančios vyriausybės prieigos prie jų duomenų. Šie apribojimai oficialiai netaikomi užsieniečiams, nors JAV vyriausybės pareigūnai viešuose ir privačiuose susirinkimuose su DG29 atstovais ne kartą tvirtino, kad minimalios informacijos procedūrų taikymo sritis buvo išplėsta taip, kad apimtų visus asmenis, nepriklausomai nuo jų tautybės ar nuolatinės gyvenamosios vietos.

702 skyriuje nurodyta, kad leistinas rinkimas „turi būti vykdomas pagal Jungtinių Amerikos Valstijų Konstitucijos Ketvirtąją pataisą, apribojančią duomenų rinkimą tiek, kiek tai atitinka pagrįstos paieškos principą. Šiuo atžvilgiu JAV ir ne JAV bendrovės neišskiriamos“. Kitaip tariant, su sąlyga, kad Ketvirtoji pataisa galioja visiems duomenims, surinktiems JAV, JAV vykdomas „masinis“ duomenų rinkimas būtų „nepagrįstas“ ir todėl prieštaraujantis Konstitucijai.

DG29 palankiai vertina PCLOB ataskaitoje pateiktas išvadas, kad „praktiškai „ne JAV asmenys“ taip pat gauna naudos iš prieigos ir saugojimo apribojimų, reikalaujamų vykdant įvairių įstaigų minimalios informacijos ir (arba) tikslo nustatymo procedūras dėl JAV asmenų informacijos identifikavimo ir pašalinimo kainos ir sudėtingumo, esant dideliame duomenų kiekiui, reiškia, kad įprastai visas duomenų rinkinys yra tvarkomas remiantis aukštesniais JAV duomenų standartais“.

Be to, DG29 pažymi, kad remiantis PCLOB išvadomis, „programa neveikia masiškai renkant pranešimus“. ODNI išleistoje 2014 metų statistinėje skaidrumo ataskaitoje ši išvada

⁴⁷ „Privatumo skydo“ VI priedas, Nacionalinės žvalgybos direktoriaus biuro (ODNI) raštas apie JAV nacionalinio saugumo įstaigoms taikomas saugumo priemones ir apribojimus, 4 p.; DG29 primena apie *ad hoc* ES ir JAV duomenų apsaugos darbo grupės ES pirmininkų ataskaitą, kurioje tvirtinama, kad „ryšių duomenys sudaro labai mažą pasaulinio interneto ryšio srauto dalį“, atsižvelgiant į tai, kad „didžioji pasaulinio interneto srauto dalis susideda iš didelės apimties srauto ir atsisiuntimų, pvz., televizijos serialai, filmai ir sportas“ (ataskaitos 3.1.2 sk.)⁴⁴

patvirtinama. Be to, remiantis PCLOB ataskaita, „sekami įrenginiai“, pvz., elektroninio pašto adresas ar telefono numeris, naudojami apibrėžiant stebėjimo tikslą⁴⁸.

Atitinkamos viešosios tikslo nustatymo taisyklės nėra tokios tikslingai suderintos taisyklės, o jų tikslas yra tik išvengti JAV asmenų arba JAV įsikūrusių asmenų sekimo. Be to, nauda, kurią, PCLOB nuomone, gauna ne JAV asmenys, praktiškai nėra privaloma ar reglamentuota teisės aktuose, kadangi su sekimu susijusiuose teisės aktuose nepateikiamos tikslingos taisyklės ir jų tikslas yra tik išvengti JAV asmenų ir JAV įsikūrusių asmenų sekimo.

Be to, DG29 primena, kad pagal 702 skirsnį asmenys yra ne tik individai, bet ir jų grupės, subjektai, asociacijos, korporacijos ar užsienio valstybės. Be to, dėl to, kad duomenų rinkimas pateisinamas „svarbiu įsigijimo tikslu, siekiant gauti užsienio žvalgybos informacijos“, jo tikslas ir reikalingumas yra neaiškus. Tačiau DG29 palankiai vertina VI priede pateiktą informaciją, kad bendras pagal 702 skyrių 2014 metais sekamų asmenų skaičius buvo apytiksliai 90 000⁴⁹. Pirmoji „privatumo skydo“ peržiūra suteiks galimybę pateikti kitus sekimo taisyklių įrodymus.

Iki šiol nėra nusistovėjusios teismų praktikos masinio ir plataus masto duomenų rinkimo srityje bei dėl vėlesnio asmens duomenų naudojimo, siekiant kovoti su nusikaltimais, įskaitant klausimą, kokiomis aplinkybėmis asmens duomenys gali būti renkami ir naudojami. Tikimasi, kad ESTT nors kažkiek išspręs šį klausimą 2016 metais sujungtose bylose *Tele2 Sverige AB / Post- och telestyrelsen* ir *Secretary of State for the Home Department / Davis ir kt.*⁵⁰ ir rekomendacijoje dėl PNR susitarimo su Kanada galiojimo.⁵¹ Tuo tarpu DG29 primena, kad ji visada manė, jog bet koku atveju masinis ir plataus masto duomenų rinkimas negali būti laikomas proporcingu.⁵²

3.3.3 Išvada

Nepaisant priėmus PPD-28 įvestų apribojimų, DG29 vis dar yra susirūpinusi dėl duomenų rinkimo proporcingumo. Visų pirma, yra požymių, kad JAV ir toliau masiškai ir plačiu mastu rinks duomenis arba bent neatmeta, kad tai darys ateityje. DG29 visada laikėsi nuoseklios pozicijos, kad toks duomenų rinkimas neatitinka ES įstatymų ir todėl yra nepriimtinas.

Antra, DG29 pažymi, kad tikslinis duomenų tvarkymas arba duomenų tvarkymas, kuris yra „kuo tikslingesnis“, gali būti laikomas masiniu. Tai, ar toks masinis duomenų rinkimas turėtų būti leistinas, ar ne, šiuo metu svarstoma ESTT. Dėl šios priežasties DG29 galutinai neįvertins tikslinio, tačiau masinio duomenų tvarkymo. Tačiau ji pabrėžia, kad jeigu būtų leidžiamas tikslinis, tačiau masinis duomenų tvarkymas, sekimo principai turėtų būti taikomi duomenų rinkimui ir vėlesniam naudojimui ir negali apsiriboti tik naudojimu. Bet koku atveju reikalingas sprendimo dėl tinkamumo projekto paaiškinimas, atsižvelgiant į šešis tikslus,

⁴⁸ PCLOB ataskaita apie stebėjimo programą, vykdytą pagal FISA 702 skyrių, 32 p.

⁴⁹ VI priedas, 11 p.

⁵⁰ ESTT, sujungtos bylos C-203/15 ir C-698/15.

⁵¹ ESTT, A-1/15 byla.

⁵² DG215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

išvardytus PPD-28, kuriais duomenys gali būti renkami „masiškai“. Šiame etape DG29 nėra įsitikinusi, kad šie tikslai pakankamai apriboti, kad būtų užtikrinta, jog duomenys renkami tik tiek, kiek tai reikalinga ir proporcinga.

3.4 C garantija: turėtų būti sukurtas nepriklausomas priežiūros mechanizmas

JAV nėra vienos priežiūros institucijos, kuriai pavesta prižiūrėti žvalgybos ir stebėjimo programų daromą poveikį privatumui ir duomenų apsaugai federaliniu lygiu. Greičiau vykdomas daugialypis JAV žvalgybos veiklos priežiūros procesas: galima išskirti vidinę ir išorinę priežiūrą. DG29 pripažįsta, kad JAV priežiūros institucijos teikia labai išsamias ataskaitas ir dažniausiai jos yra viešos.

3.4.1 Vidinė priežiūra

Visose žvalgybos ir saugumo įstaigose dirba darbuotojai, kurie yra atsakingi už teisės nuostatų laikymąsi, įskaitant generalinius inspektorius, kurių pagrindinis uždavinys yra įvertinti bendrą įstaigų darbo atitiktį teisės aktams, įskaitant su privatumu ir duomenų apsauga susijusius įstatymus, tačiau jais neapsiribojant. Generaliniai inspektoriai numatyti įstatyme; jie yra (arba greitai bus) skiriami prezidento ir tvirtinami senato, siekiant užtikrinti, kad organizaciniu požiūriu jie būtų nepriklausomi ir atskaitingi Kongresui. DG29 mano, kad generaliniai inspektoriai atitiks organizacinės nepriklausomybės kriterijų, kaip apibrėžta ESTT ir Europos žmogaus teisių teismo (EŽTT), bent nuo tada, kai visiems pradeda galioti naujas kandidatų nominavimo procesas. Šiuo metu lieka keli susirūpinimą keliantys klausimai dėl generalinių inspektorių, kurie vis dar skiriami agentūros, kurią jie prižiūri, direktoriaus.

Generaliniai inspektoriai gali teikti rekomendacijas, kurios gali būti perduotos Teisingumo departamentui ir PCLOB arba netgi Kongreso komitetui, kurie gali įgyvendinti tas rekomendacijas. Jeigu generalinis inspektorius nustato pažeidimą, jis gali būti pašalintas imantis vidinių ir politikos priemonių, o ataskaita apie tai teikiama Kongresui. Generalinis inspektorius gali, pavyzdžiui, atlikti auditą ir patikrinimus.

DG29 pažymi, kad generalinio inspektoriaus ataskaitos viešai neskelbiamos ir kad generaliniam inspektoriui taip pat gali būti draudžiama teikti ataskaitas, jeigu tikrinama informacija yra įslaptinta. Tačiau ataskaitos visada prižiūrimos Kongreso ir tai yra esminė saugumo priemonė, netgi jeigu nėra individualaus teisių gynimo pagrindų.

Visose agentūrose yra privatumo ir pilietinės laisvės pareigūnai, kurie teikia su privaloma atsiskaitymo sistema susijusią pagalbą prižiūrint Kongresui.

Apskritai vidinės priežiūros mechanizmai gali būti laikomi pakankamai patikimais; tačiau, kad būtų galima pateisinti kišimąsi į pagrindines teises į privatumą ir duomenų apsaugą, priežiūra turi būti visiškai nepriklausoma. Nors DG29 gerbia ir vertina įvairių privatumo ir pilietinės laisvės pareigūnų darbą, ji negali daryti išvados, kad jie atitinka reikiamą nepriklausomumo veikti kaip nepriklausomiems priežiūros pareigūnams lygį.

3.4.2 Išorinė priežiūra

Išorinė priežiūra susideda iš įvairių mechanizmų: teisminės priežiūros pagal 501 ir 702 skyrių, užtikrinamos FISA teismo (toliau: FISC), specialių Kongreso žvalgybos komitetų priežiūros ir PCLOB vykdomų užduočių.

DG29 primena, kad, kaip nurodė ESTT ir EŽTT, siekiant užtikrinti nepriklausomybę ir procedūros nešališkumą idealiu atveju priežiūrą turėtų vykdyti teisėjas. Iki šiol FISC procedūra buvo *ex parte* procedūra, nesuteikianti galimybių, kad susiję asmenys būtų išklaustyti arba netgi žinotų apie bylą. Taip pat ir šiandien FISC procedūra išlieka *ex parte*, tačiau priėmus JAV LAISVĖS aktą, FISC buvo pristatyti *amici curiae*. *Amici curiae* veikia nepriklausomai, tačiau jų paskirtis nėra ginti tam tikrus asmenis, kurie gali būti susiję su byla.

Pagal JAV laisvės aktą buvo sukurta *amici curiae* grupė, teiksianti pareiškimus apie svarbius atvejus FISC. Teismas atrinko penkis advokatus, kurie gavo atitinkamus saugumo leidimus ir teikia technines rekomendacijas, lanko FISC posėdžius ir teikia pranešimus bei įrodinėja bylos aplinkybes iš privatumo ir pilietinių teisių perspektyvos. Tačiau jie tai atliks tik svarbiose bylose arba kai iškyla naujų teisinių klausimų.⁵³

215 skyriui beveik visa apimtimi taikoma *ex ante* (tačiau ne *ex post*) teisminė priežiūra, kadangi visos programos, kai kaip duomenų rinkimo pagrindas naudojamas 215 skyrius, turi būti patvirtintos FISC. PCLOB ataskaitoje nurodyta, kad „702 skyrius skiriasi nuo šios tradicinės FISA elektroninio stebėjimo sistemos tiek taikomų standartų, tiek individualių FISC nuostatų trūkumo atžvilgiu. Pagal statutą generalinis prokuroras ir nacionalinės žvalgybos direktorius atlieka metinį sertifikavimą, suteikiant galimybes sekti ne JAV asmenis, kurie tikėtina yra už Jungtinių Amerikos Valstijų ribų, siekiant gauti užsienio žvalgybos informacijos, FISC nenurodant konkrečių ne JAV asmenų, kurie bus sekami. [...] Taip pat nėra reikalavimo, kad vyriausybė nurodytų galimą priežastį, kuria vadovaujantis galima teigti, jog 702 skyriaus objektas yra užsienio jėgos arba užsienio jėgų atstovas, kaip reikalaujama pagal tradicinę FISA.“⁵⁴

Kongrese specialūs žvalgybos komitetai privalo atlikti priežiūrą ir patvirtinti žvalgybos veiklą, tiksliau, balsuojant už biudžetą. Senatas ir vietos žvalgybos komitetai gauna įslaptintus pranešimus apie žvalgybos veiklą. AG šiems komitetams turi teikti ataskaitas apie elektroninę FISA stebėjimą kas šešis mėnesius. DG29 vis dar neaišku, kiek jie gali aptarti asmenų duomenų tvarkymą, ypač jei jie yra ne JAV asmenų.

PCLOB yra nepriklausoma JAV vyriausybės vykdomosios valdžios dalis, kuriai suteikti du pagrindiniai įgaliojimai: (1) peržiūrėti ir analizuoti veiksmus, kuriuos vykdomoji valdžia atlieka, siekdama apsaugoti [JAV] tautą nuo terorizmo, užtikrinant, kad tokių veiksmų poreikis suderintas su poreikiu saugoti privatumą ir pilietinę laisvę ir (2) užtikrinti, kad kuriant ir įgyvendinant įstatymus, nuostatas ir taisykles, susijusias su pastangomis, siekiant

⁵³ Laisvės aktas IV SKYRIUS--UŽSIENIO ŽVALGYBOS STEBĖJIMO TEISMO REFORMOS 401 sk. *Amici curiae* paskyrimas.

⁵⁴ PCLOB ataskaita apie stebėjimo programą pagal FISA 702 skyrių, 24, 25 p.

apsaugoti tautą nuo terorizmo, atitinkamai atsižvelgiama į su laisve susijusius klausimus. DG29 pažymi, kad PCLOB turi šaukimo į teismą įgaliojimus ir prieigą prie slaptos informacijos. Vykdydama savo funkciją, ji taip pat tikrina programų efektyvumą. Jos priežiūra nevykdoma iki fakto, o vykdoma po jo. PCLOB pademonstravo savo nepriklausomas galias, nesutikdama su Jungtinių Amerikos Valstijų prezidentu teisiniais klausimais. Tiksliau, ji manė, kad 215 skyriuje minėtai telefonų metaduomenų programai nebuvo suteiktas teisėtas leidimas, ir padarė išvadą, kad jos nepakako, kadangi nebuvo nutrauktų išpuolių įrodymų. PCLOB taip pat atliko vienerius metus trukusį 702 programos tyrimą ir nustatė, kad ji yra teisėta ir leistina pagal statutą ir kad 702 skyrius iš tikrųjų yra labai veiksmingas, įskaitant kovą su terorizmu. Galiausiai ji veikė skaidrumo reikalavimo pagrindu ir nustatė, kad įvairūs įslaptinti faktai neturėjo būti įslaptinti. Suprantama, kad PCLOB artimiausiu metu pateiks ataskaitą apie PPD-28 įgyvendinimą. Šiuo atžvilgiu ji mano, kad norint saugoti informaciją apie užsienietį, paprasčiausio fakto, kad asmuo yra užsienietis, nepakanka.

Galiausiai, DG29 pažymi, kad EO12333 nenumatyti teisminės kontrolės, priežiūros ar teisių gynimo mechanizmai šiuo pagrindu vykdomoms priežiūros programoms.

3.4.3 Išvada

Sprendimo dėl tinkamumo projekte nurodyta, kad JAV įgyvendinamas daugialypis tiek vidinės, tiek išorinės priežiūros mechanizmas. Nors priežiūros mechanizmų veikimas gali būti prieštaringas, DG29 patenkinta tuo, kad iš esmės įgyvendinama pakankamai vidinės priežiūros mechanizmų. Tačiau DG29 nuogaštauja, kad nėra pakankamai EO12333 pagrindu vykdomų priežiūros programų kontrolės.

DG29 pažymi, kad jos anksčiau kritikuota problema, kad procedūros FISC atžvilgiu nėra grindžiamos rungimusi, paskiriant *amici curiae*, kuriems pavesta „didinti asmens saugumo ir pilietinių laisvių apsaugą“, buvo sumažinta tik šiek tiek. Nepaisant to, FISC neužtikrina veiksmingos teisminės ne JAV asmenų sekimo kontrolės. Taip pat išlieka šiek tiek abejonių dėl FISC sugebėjimo efektyviai įvertinti sekimo ir minimalios informacijos procedūras, kaip tvirtino PCLOB⁵⁵.

3.5 D garantija: asmenims turi būti užtikrintos veiksmingos teisių gynimo priemonės

3.5.1 Teisminės gynybos priemonės

3.5.1.1 Ieškinio teisės reikalavimas

JAV sistemoje teisminių gynybos priemonių atžvilgiu numatytas svarbus apribojimas: remiantis JAV Konstitucija, reikalaujama, kad asmuo turėtų teisę reikšti ieškinį: „reikalavimas dėl to, kad ieškovai patyrė ar patirs tiesioginę žalą ar nuostolius ir kad šie nuostoliai gali būti atlyginti. Federaliniu lygiu teisiniai veiksmai negali būti atlikti tiesiog dėl

⁵⁵ PCLOB ataskaita dėl stebėjimo programos, vykdytos pagal FISA 702 skyrių, 11 p.

to, kad asmuo ar jų grupė yra nepatenkinti vyriausybės veiksmu ar įstatymu“⁵⁶. Pasirodo, toks reikalavimas yra panaikintas dėl pranešimo prižiūrimiems asmenims trūkumo, netgi kai šios priemonės baigtos taikyti. ESTT ir EŽTT ne kartą tvirtino, kad asmenys turi turėti prieigą prie administracinių ar teisminių teisių gynimo procedūrų. Sprendime *Zakharov* EŽTT patvirtino, kad remiantis teismo praktika, bet kas gali kreiptis į teismą, jeigu yra teisėtų priešasčių įtarti kišimasi į jų pagrindines teises⁵⁷.

Be to, remiantis Jungtinių Amerikos Valstijų aukščiausiojo teismo praktika, už JAV ribų esantiems užsieniečiams nesiūloma visiška konstitucinė apsauga JAV⁵⁸. Tai yra tiesa ypač Ketvirtosios pataisos atžvilgiu, kuria remiantis JAV piliečiai – tačiau ne ne JAV asmenys – apsaugomi nuo nepagrįstų paieškų ir areštų ir kurioje reglamentuota JAV teisė į privatumą. Europos piliečiams ir kitiems Europos asmenims, gyvenantiems už JAV ribų, Ketvirtoje pataisoje numatyta apsauga negalioja⁵⁹.

Ribotas Teisminio teisių gynimo akto taikymas (tiek iš esmės, kadangi jame nenumatytas nacionalinis saugumas, tiek asmenų, kurie gali pasikliauti įstatymais, atžvilgiu), daugybė išimčių ir teisinis neapibrėžtumas agentūrų, kurioms galioja Teisminio teisių gynimo aktas, atžvilgiu nepatenkina reikalavimo pasiūlyti veiksmingą žalos atlyginimo mechanizmą visiems susijusiems asmenims nacionalinio saugumo žvalgybos stebėjimo atvejais.

3.5.1.2 Prezidento politinė direktyva Nr. 28

DG29 pažymi, kad PPD-28 yra tik direktyva ir todėl pagal ją asmenims negali būti suteiktos jokios teisės. Tai galima padaryti tik įstatymais. Todėl asmenys negali kreiptis į teismą įtariamo PPD-28 saugumo priemonių pažeidimų pagrindu.

3.5.1.3 Užsienio žvalgybos stebėjimo aktas

Remiantis FISA, neteisėto stebėjimo atveju asmenys gali pasinaudoti keliomis teisių gynimo priemonėmis. Remiantis FISA, „nukentėjęs asmuo, kuris nėra užsienio valstybė ar užsienio valstybės agentas [...], atitinkamai, kuriam buvo taikomos elektroninio stebėjimo priemonės ar apie kurį buvo atskleista elektroninio stebėjimo priemonėmis gauta informacija ar tokia informacija buvo naudojama, pažeidžiant 1809 skyrių, turi pagrindą imtis atitinkamų veiksmų prieš asmenį, kuris įvykdė tokį pažeidimą“. Tačiau tam aiškiai nepriskiriamos užsienio valstybės ar užsienio valstybių agentai, kuriems buvo taikoma atitinkama priemonė. Nepaisant to, kaip nurodyta pirmiau, ieškovas turės įrodyti, kad turi teisę reikšti ieškinį, kuris praktiškai nebus įmanomas.

Remiantis JAV laisvės aktu, buvo sukurta *amicus curiae* patariamoji grupė, kuri FISA teismui teiks (neprivalomas) rekomendacijas svarbaus naujo teisinio aiškinimo atveju. Tačiau jų

⁵⁶ <https://www.law.cornell.edu/wex/standing>;

<https://www.law.cornell.edu/wex/standing><https://www.law.cornell.edu/wex/standing>; *Clapper prieš Amnesty International USA*

⁵⁷ EŽTT, *Zakharov*, 171 sk.

⁵⁸ U.S. / *Verdugo – Urquidez*, 264–266 p.

⁵⁹ ES pirmininkų ataskaita, 2 skyrius.

užduotis yra teikti nešališkas rekomendacijas, o ne ginti konkretaus asmens interesus jo prašymu.

3.5.2 Administracinės teisių gynbos priemonės

3.5.2.1 Generaliniai inspektoriai

Kitas teisių gynimo būdas yra veikti per generalinį inspektorių, kuriam gali būti pateiktas skundas. Tačiau generaliniai inspektoriai nėra įsipareigoję svarstyti kiekvieną skundą: teisė būti išklausytam nesuteikiama, greičiau suteikiami diskreciniai įgaliojimai. Generalinis inspektorius taip pat gali teikti ataskaitas, kuriose pateiktos išvados apie pažeidimus informacijos išslaptinimo atveju. Jeigu asmuo mano, kad ataskaita jam pakenks, jis gali kreiptis į teismą dėl įstatymų pažeidimo.

3.5.2.2 Informacijos laisvės aktas

Visiems asmenims užtikrinama teisių gynimo priemonė yra informacijos laisvės prašymo pateikimas, remiantis Informacijos laisvės aktu (FOIA). JAV vyriausybės teigimu, FOIA prašymas iš esmės gali būti pateiktas bet kokio asmens – tiek JAV piliečio, tiek ne JAV piliečio – paprasčiausiai prašant agentūros įrašo. Tai galioja ir įrašams apie asmenį, nors tokiu atveju reikalaujama pateikti asmens tapatybės patvirtinimą. Tačiau jeigu informacija išlaptinta siekiant užtikrinti nacionalinį saugumą, mažai tikėtina, kad FOIA prašymas bus sėkmingas, kadangi taikoma išimtis: agentūros neprivalo suteikti prieigą prie išlaptintos informacijos, įskaitant tuos atvejus, jeigu ta informacija yra susijusi su asmeniu, kuris pateikė prašymą. Vykdomų teisėsaugos tyrimų informacija neįtraukiama į FOIA prašymus. Galiausiai, DG29 supratimu FOIA prašymas nesuteikia teisės reikalauti, kad nepriklausoma institucija patikrintų duomenų tvarkymo teisėtumą.

3.5.3 „Privatumo skydo“ ombudsmenas

3.5.3.1 Ombudsmeno skyrimas

„Privatumo skyde“ numatytas naujas mechanizmas ES asmenims teikti prašymus dėl JAV signalų žvalgybos naujai paskirtam „privatumo skydo“ ombudsmenui. Kaip paaiškinta memorandume, pridėtame prie valstijos sekretoriaus John Kerry 2016 m. vasario 22 d. rašto, ombudsmeno pareigas eis sekretoriaus pavaduotoja C. Novelli. Ji eis tas pareigas papildomai prie tarptautinės informacinių technologijų demokratijos vyresniosios koordinatorės pareigų, kurios numatytos PPD-28 4 skyriaus d dalyje. Rašte ir memorandume pabrėžiama, kad „sekretoriaus pavaduotoja yra atskaitinga tiesiogiai valstijos sekretoriui ir yra nepriklausoma nuo žvalgybos bendruomenės“.

Nepaisant pareigų pavadinimo, memorandume paaiškinta, kad „privatumo skydo“ ombudsmenas ne tik nagrinės prašymus dėl nacionalinio saugumo prieigos prie duomenų, perduodamų iš ES į JAV pagal „privatumo skydą“, bet ir kai duomenys perduodami pagal standartines sutarties sąlygas, privalomas įmonių taisyklės, išimtis (pagal Direktyvos

95/46/EB 26 straipsnį) arba „galimas būsimas išimtis“, kaip nurodyta memorandumo 2 išnašoje.

Tikimasi, kad mechanizmas veiks tokiu būdu: ES asmuo pateikia prašymą nacionalinio saugumo paslaugų priežiūros srityje kompetentingai valstybės narės įstaigai ar centralizuotai ES asmenų skundų nagrinėjimo įstaigai, jeigu tokia įstaiga bus įkurta ar paskirta. Visų pirma, ombudsmenui prašymą siunčianti įstaiga privalo patikrinti, ar pateiktas tinkamas prašymas, kaip nurodyta rašto 3 skirsnio b dalyje⁶⁰. Kai prašymas perduodamas „privatumo skydo“ ombudsmenui ir nustatoma, kad jis atitinka 3 skirsnio b dalį, „privatumo skydo“ ombudsmenas pateikia atsakymą, t. y. jis galutinai patvirtina, kad „(i) skundas buvo tinkamai išnagrinėtas ir (ii) kad atitinka JAV įstatymus, statutus, vykdomuosius įsakus, prezidentinės direktyvas ir agentūrų taisykles, kuriose numatyti apribojimai ir saugumo priemonės, aprašytos nacionalinės žvalgybos direktoriaus biuro (ODNI) rašte, arba jeigu jis neatitiko nurodytų nuostatų, toks neatitikimas buvo pašalintas“⁶¹. Atsakymu „nei patvirtinama, nei paneigiama, ar asmuo buvo stebėjimo objektas, be to „privatumo skydo“ ombudsmenas nepatvirtina, kad buvo taikomos specialios teisių gynimo priemonės“⁶². Klausiant, kaip atliekamas ombudsmeno tyrimas, paaiškinama, kad „privatumo skydo“ ombudsmenas „glaudžiai bendradarbiaus su kitais Jungtinių Amerikos Valstijų vyriausybės pareigūnais, įskaitant atitinkamas nepriklausomas priežiūros įstaigas“⁶³, o tiksliau, „galės glaudžiai bendradarbiauti su ODNI, Teisingumo departamentu ir kitais departamentais ir agentūromis, susijusiomis su Jungtinių Amerikos Valstijų nacionaliniu saugumu, bei generaliniais inspektorais, informacijos laisvės akto pareigūnais ir už pilietinės laisvės ir privatumą atsakingais pareigūnais“⁶⁴. Toks bendradarbiavimas turi užtikrinti, kad „privatumo skydo“ ombudsmenas gali siųsti atsakymą, įskaitant pirmiau nurodytus patvirtinimus.

3.5.3.2 Naujo ombudsmeno mechanizmo įvertinimas

Darbo grupė pripažįsta Europos Komisijos ir JAV vyriausybės pastangas, siekiant įvesti naują mechanizmą, kad pagerintų teisių gynimo priemonių galimybes JAV stebėjimo veiklos atžvilgiu. Ji supranta, kad šio mechanizmo kaip naujienos tarptautinių ryšių signalų stebėjimo ar nacionalinio saugumo srityje įvertinimas yra ypač svarbus.

⁶⁰ b. ES asmens skundą nagrinėjanti įstaiga, atlikdama žemiau nurodytus veiksmus, užtikrina, kad prašymas būtų išsamus:
(i) Patikrindama asmens tapatybę ir kad asmuo veikia savo vardu, o ne kaip valdžios įstaigos ar tarptautinės organizacijos atstovas.

(ii) Užtikrindama, kad reikalavimas pateiktas raštu ir kad jame pateikta ši pagrindinė informacija:

- informacija, kuri yra prašymo pagrindas,
- informacijos pobūdis ar prašomos ištaisomosios priemonės,
- tikėtina susijusios Jungtinių Amerikos Valstijų įstaigos, jei tokių yra, ir
- kitos priemonės, kurių imamasi, siekiant gauti informacijos ar prašytų ištaisomųjų priemonių, ir atsakymas, gautas taikant tas kitas priemones.

(iii) Patikrindama, kad prašyme pateikti duomenys, kurie galėjo būti perduoti iš ES į Jungtines Amerikos Valstijas pagal „privatumo skydą“, standartines sutarčių nuostatas, įmonėms privalomas taisykles, išimtis ar galimas būsimas išimtis.

(iv) Nustatydama, kad prašymas nėra nerimtas, nepagrįstas ar pateiktas nesąžiningai.

⁶¹ „Privatumo skydas“, III priedas, 4.e skyrius.

⁶² „Privatumo skydas“, III priedas, 4.e skyrius.

⁶³ „Privatumo skydas“, III priedas, 2.a skyrius.

⁶⁴ „Privatumo skydas“, III priedas, 2.a skyrius.

Šiame skyriuje DG29 įvertins, kaip „privatumo skydo“ ombudsmeno paskyrimas yra susijęs su būtinais reikalavimais asmenims kreiptis dėl žalos atlyginimo, kaip nurodyta Chartijoje, EŽTK ir Europos teismų praktikoje.

3.5.3.3 Ar gali pakakti vien ombudsmeno paskyrimo ?

Iš pradžių reikia užduoti klausimą, ar „ombudsmeno“ paskyrimas gali būti laikomas atitinkančiu Chartijos 47 straipsnį – kuriame nurodyta veiksminga teisių gynbos nešališkame teisme priemonė⁶⁵ – bent jau, jeigu kitas būdas nėra galimas, siekiant veiksmingo teisėto žalos atlyginimo. Tai yra svarbu, kadangi ESTT Schrems bylos svarbiame 95 teiginyje mini Chartijos 47 straipsnį, tačiau nenurodo, kad 47 straipsnis turi būti suprantamas, atsižvelgiant į pakeitimus stebėjimo priemonių kontekste. Priešingai, ESTT jau taikė Chartijos 47 straipsnį Kadi II byloje⁶⁶ atitinkamai nacionalinio ir tarptautinio saugumo priežiūros priemonių atžvilgiu⁶⁷.

Remiantis EŽTT praktika, akivaizdu, kad teisinės teisių gynimo priemonės įprastuose teismuose nėra sąlyga, pagal kurią svarstoma, ar stebėjimo schemos atitinka 8 straipsnį (ir EŽTK 13 straipsnį)⁶⁸. Teismas išaiškino 8 straipsnį kaip būtiną stebėjimo veiklos apsaugos priemonę, kad žalos atlyginimas kitų institucijų atžvilgiu būtų tinkamas. Nepaisant to, EŽTT deda daug vilčių, kad kitos institucijos užtikrins veiksmingas teisių gynimo priemones, tvirtindama, kad tokia institucija turi būti „nepriklausoma nuo valdžios įstaigų, kurios vykdo stebėjimą, ir jai suteikta pakankamai galių ir kompetencijos vykdyti veiksmingą ir tęstinę kontrolę“⁶⁹.

Kennedy ir *Klass* byloje EŽTT apžvelgė, ką tokie lūkesčiai galėtų reikšti slapto stebėjimo kontekste, kai duomenų subjektui nepranešama apie jo duomenų tvarkymą. Abiejuose sprendimuose EŽTT valdžios įstaigas laikė nepriklausomomis, ypač nepriklausomomis nuo stebėjimą vykdančių institucijų ir nuo kitų įstaigų nurodymų⁷⁰. Tiksliau, *Kennedy* byloje teismas pritarė nepriklausomai ir nešališkai įstaigai, kuri priėmė savo darbo tvarkos taisykles ir kuri buvo sudaryta iš narių, kurie užėmė ar anksčiau užėmė aukštas pareigas teismo institucijose arba buvo patyrę teisininkai⁷¹.

⁶⁵ Be to, Pagrindinių teisių chartijos paaiškinimuose nurodyta, kad 47 straipsnis turi būti aiškinamas kaip suteikiantis teisės į veiksmingas teisių gynbos priemones teisme garantiją (Pagrindinių teisių chartijos paaiškinimas, 47 straipsnio paaiškinimas (2007/C 303/02)).

⁶⁶ 2013 m. liepos 18 d. sprendimas sujungtose bylose, *European Commission and United Kingdom / Kadi*, C-584/10 P, C-593/10 P ir C-595/10 P

⁶⁷ *Kadi* II 97 ir 100 sk.: visų Sąjungos aktų, įskaitant tuos, pagal kuriuos įgyvendinami Saugumo tarybos patvirtinti sprendimai pagal Jungtinių Tautų chartijos VII skyrių, teisėtumas svarstomas Europos Sąjungos teismų (VII skyriuje reglamentuojami veiksmai, kovojant su taikai kylančiomis grėsmėmis, taikos pažeidimais ir agresijos veiksmais).

⁶⁸ Remiantis EŽTK 13 straipsniu, valstybės narės įpareigojamos užtikrinti, kad „visi, kieno teisės ir laisvės (...) pažeidžiamos, galės pasinaudoti veiksmingomis teisių gynimo priemonėmis nacionalinės valdžios institucijos atžvilgiu“. Tai neturi būti teismo institucija, kaip EŽTT paaiškino *Klass* 56 ir 67 sk.

⁶⁹ *Klass* 56 ir 67 sk.

⁷⁰ EŽTT, *Klass* 21 ir 53 sk.

⁷¹ G 10 komisija (sprendimo priėmimo metu) buvo sudaryta iš trijų narių, iš kurių pirmininkas turi būti kompetentingas eiti pareigas teismo institucijose, *Klass* 21 ir 53 sk.)

Nagrinėdamos asmenų skundus, valdžios įstaigos, priimdamos abu sprendimus, turėjo prieigą prie visos svarbios informacijos, įskaitant slaptą medžiagą. Galiausiai, jos abi buvo kompetentingos ištaisyti trūkumus⁷².

Be klausimo, ar ombudsmenas gali būti laikomas „teismu“, Chartijos 47 straipsnio 2 dalies taikymas kelia papildomų iššūkių, kadangi joje nurodyta, kad teismas turi būti skiriamas „įstatymų nustatyta tvarka“. Tačiau kyla abejonių, ar memorandumas, kuriame nustatytas naujojo mechanizmo veikimas, gali būti laikomas „įstatymu“.

Dėl to – atsižvelgdama į esminį lygiavertiškumą, užuot vertinusi, ar ombudsmenas formaliai gali būti laikomas įstatymuose numatyta tvarka paskirtu teismu, darbo grupė nusprendė toliau tobulinti teismų praktikos niuansus konkrečių reikalavimų, būtinų svarstant „teisines teisių gynybos priemones“ ir „teisinio žalos atlyginimo priemones“, atžvilgiu, remiantis pagrindinėmis teisėmis, numatytomis Chartijos 7, 8 ir 47 straipsnyje ir EŽTK 8 (ir 13) straipsnyje. Atlikdama išsamesnę analizę ir aptardama naujojo mechanizmo taikymo apimtis, darbo grupė didelį dėmesį skirs šiems kriterijams: reikalavimui pateikti prašymą ombudsmenui ir gauti atsakymą („teisė teikti ieškinį“), ombudsmeno nepriklausomybei, jo tyrimo įgaliojimams prieiti prie reikalingos medžiagos, įskaitant įslaptintus dokumentus ir prašyti pagalbos kitų agentūrų ir, galiausiai, įgaliojimams trūkumams šalinti.

3.5.3.4 Ombudsmeno mechanizmo taikymo apimtis

Atsižvelgdama į prieigą prie ombudsmeno mechanizmo, DG29 mano, kad visi asmenys, kuriems galioja ES įstatymai, turėtų galėti pasinaudoti saugumo priemonėmis pagal „privatumo skydą“. Būtų nepriimtina nustatyti skirtumus, remiantis tautybe, ypač atsižvelgiant į tai, kad pagrindinės teisės ES galioja visiems, o ne tik tiems, kas turi ES pasą. III priede minimas „ES asmuo“, toliau neapibrėžiant, kas jis yra. Darbo grupė apgailestauja dėl tokio neapibrėžtumo ir rekomenduoja teikti paaiškinimus, kad visi asmenys, kuriems galioja ES įstatymai, turi teisę, kad jų prašymai ombudsmenui būtų nagrinėjami pagal memorandumo sąlygas. Be to, Komisija ir JAV turėtų išspręsti klausimą, kiek „privatumo skydas“ galios EEE šalių ir Šveicarijos piliečiams / gyventojams, kuriems anksčiau galiojo „saugaus uosto“ sistema.

Be to, DG29 pažymi, kad yra neaiškumų dėl ombudsmeno mechanizmo taikymo apimties. Kadangi memorandume nurodyta, kad ombudsmenui pavesta nagrinėti prašymus, susijusius su duomenų, perduotų iš ES į JAV, nacionaliniu saugumu, atsižvelgiant į visus perdavimo įrankius, prieinamus pagal ES įstatymus, memorandume aiškiai nurodyta, kad numatomas mechanizmas „dėl signalų žvalgybos“. Pastarasis terminas reiškia, kad tai galioja tik tokiam duomenų perdavimui, kai duomenys surenkami, pasitelkiant signalų žvalgybos priemones, dėl ko kyla klausimas, ar, pavyzdžiui, pagal FISA surinkti duomenys laikomi „signalų žvalgyba“. Taip yra 702 skyriaus atveju, kaip paaiškinta ODNI pareiškime, 10 p⁷³. Tačiau DG29 apgailestauja, kad termino „signalų žvalgyba“ naudojimas šiuo atžvilgiu sukelia bereikalingo neapibrėžtumo.

⁷² EŽTT, Kennedy 167 sk.; *Klass* 21 ir 53 sk.

⁷³ „Privatumo skydas“, VI priedas, 10 p.

Kitas svarbus aspektas yra darbo grupės tvirtinimas, kad ombudsmeno mechanizmas neapima prašymų, susijusių su teisėsaugos agentūrų prieiga⁷⁴. Jeigu taip yra, liktų neaišku, ar šis mechanizmas galėtų būti taikomas kai kurių agentūrų prašymams, ypač CŽV.

3.5.3.5 Teisė reikšti ieškinį ir prašymų teikimo tvarka

Labai sudėtinga pateikti ieškinį dėl stebėjimo priemonių įprastuose Jungtinių Amerikos Valstijų teismuose. Darbo grupė žino, kad aukščiausiasis teismas nesuteikė teisės pareikšti ieškinį žvalgybos byloje, jeigu pareiškėjas negalėjo pateikti „konkrečių, tikslų ir faktinių ar neišvengiamų ar žalos įrodymų“⁷⁵. Šiuo atžvilgiu ombudsmeno skyrimas yra svarbus žingsnis, kadangi tai yra dar viena teisinė žalos atlyginimo priemonė, kurios priešingu atveju nebūtų. Todėl darbo grupė teigiamai vertina 3 skyriaus c dalyje pateiktą paaiškinimą. Remiantis šiuo skyriumi, įrodymų, kad buvo pasinaudota prieiga prie prašančiojo duomenų, pasitelkiant signalų žvalgybos priemones, nereikia norint pateikti prašymą, naudojantis nauju mechanizmu.

Darbo grupė didžiaja dalimi pritaria skundo teikėjo identifikavimo procedūrai, naudojantis ombudsmeno mechanizmu. Būtų išmintinga identifikavimą vykdyti ES teritorijoje kaip ir prieigos mechanizmo pagal ES ir JAV TFTP2 sutartį atveju. Tačiau darbo grupė nesupranta, kodėl patikrinimas ES turėtų būti atliekamas „valstybių narių, kurios yra kompetentingos vykdyti nacionalinio saugumo tarnybų priežiūrą“. Visų pirma, nepanašu, kad remiantis Sutarties dėl Europos Sąjungos 4 straipsnio 2 dalimi, Europos Komisija galėtų šioms institucijoms skirti užduotis, kurios akivaizdžiai yra valstybių narių kompetencijos ribose.

Be to, atsižvelgiant į nacionalinio saugumo tarnybų priežiūros mechanizmų įvairovę valstybėse narėse, atitinkamų valdžios įstaigų dalyvavimas gali žymiai įtakoti valstybių narių piliečiams skirtos sistemos efektyvumą. Pavyzdžiui, tais atvejais, kai yra kelios valdžios įstaigos, kurios yra atsakingos už nacionalinio saugumo tarnybų priežiūrą ir gali būti sudėtinga asmeniui nustatyti, kuri yra svarbi, kai galiojančiose nacionalinėse teisės nuostatose nenumatyta galimybė asmenims susisiekti su atitinkama priežiūros įstaiga arba jeigu tos valdžios įstaigos nėra įsteigtos tokiu būdu, kad galėtų vykdyti joms pagal sprendimo dėl tinkamumo projektą priskirtas funkcijas⁷⁶. Atsižvelgiant į DAI dalyvavimą taikant ir prižiūrint „privatumo skydą“ bei jų panašų vaidmenį pagal TFTP2 sutartį, labiau tikslinga šią užduotį priskirti valstybių narių nacionalinėms duomenų apsaugos įstaigoms. Darbo grupė pabrėžia, kad ji mano, jog mažai tikėtina, kad įslaptinta informacija tvarkoma kaip „privatumo skydo“ ombudsmeno procedūros dalis, kadangi bet kokie atsakymai bus tik „tinkami ar netinkami, tačiau ištaisyti“.

3.5.3.6 Nepriklausomybė

Remiantis valstijos sekretoriaus pranešimais, akivaizdu, kad ombudsmeno pareigas eis valstijos departamento sekretoriaus pavaduotojas. Ombudsmenas skiriamas prezidento, o jo

⁷⁴ Memorandumas dėl ombudsmeno skyrimo, 1 p.

⁷⁵ Clapper / Amnesty International USA, 568 U.S. ____ (2013) II, 10 p.

⁷⁶ Pavyzdžiui, kai kuriose ES valstybėse narėse asmenys gali gauti prieigą prie nacionalinio saugumo tarnybų saugomos informacijos, pateikę prašymą Aukščiausiam teisingumo teismui.

paskyrimas patvirtinamas senato. Ombudsmeno pareigybių nereikia papildomai patvirtinti, pakanka priskirti ombudsmeno pareigas. Sekretoriaus pavaduotojas skiriamas JAV prezidento, jam kaip ombudsmenui nurodymus duoda valstijos sekretorius, o kandidatūrą patvirtina JAV senatas, atstovaujamas sekretoriaus pavaduotojo. Kaip nurodyta rašte ir memorandume, ombudsmenas yra „nepriklausomas nuo JAV žvalgybos bendruomenės“. Tačiau DG29 abejoja, ar ombudsmeno pareigybės sukurtos tinkamiausiame departamente. Siekiant efektyviai eiti ombudsmeno pareigas, būtinos tam tikros žinios ir supratimas apie žvalgybos bendruomenės veiklą, tačiau tuo pat metu iš tikrųjų būtinas pakankamas atstumas nuo žvalgybos bendruomenės, kad jis galėtų veikti nepriklausomai.

„Privatumo skyde“ nenumatyti specialūs ombudsmeno atleidimo kriterijai. Darbo grupė mano, kad ombudsmenas gali būti atleistas iš ombudsmeno pareigų tokiu pat būdu kaip ir Valstybės departamento sekretoriaus pavaduotojo pareigų, kas gali pakenkti nepriklausomoms ombudsmeno pareigoms.

Iš pirmo žvilgsnio, Valstybės departamento sekretoriaus pavaduotojo paskyrimas ombudsmenu akivaizdžiai skiriasi nepriklausomybės nuo įprasto teismo jurisdikcijos nustatymo teisinio asmens patirtos žalos atlyginimo tikslais atžvilgiu. Iškyla klausimas, ar nepriklausomybės atžvilgiu ombudsmenas gali būti laikomas lygiu kitoms nepriklausomoms priežiūros įstaigoms, kurios atitinka reikalavimus. Stebėjimo atžvilgiu, tai būtų Tyrimo įgaliojimų teismas (TIT) JK ir G10 komisija Vokietijoje.

Reikia papildomai įvertinti, ar taip yra, atliekant „nepriklausomam subjektui“ suteiktų įgaliojimų analizę.

3.5.3.7 Tyrimo įgaliojimai

Atsižvelgdamas į Chartijos 47 straipsnį, *Kadi II* byloje ESTT nusprendė, kad „asmuo turi galėti nurodyti priežastis, kuriomis pagrįstas jo atžvilgiu priimtas sprendimas, atsižvelgiant į patį sprendimą arba reikalaujant atskleisti tas priežastis ir gaunant leidimą, nepažeidžiant teismo, kuris yra kompetentingas reikalauti atitinkamų įgaliojimų atskleisti tą informaciją, įgaliojimų, kad jis galėtų ginti savo teises geriausiomis sąlygomis“⁷⁷. Europos Sąjungos teismai privalo užtikrinti, kad tas sprendimas priimamas pakankamai svarių faktinių pagrindų⁷⁸. Aiškiai nurodyta, kad „[...] informacijos ar įrodymų slaptumas ar konfidencialumas nėra svarus prieštaravimas“, bent jau Europos Sąjungos teismuose⁷⁹. Todėl darbo grupė tvirtina, kad ombudsmenui turi būti pateikta informacija ir įrodymai, kurie pagrindžia priemonės taikymo priežastis, siekiant patenkinti ESTT reikalavimus⁸⁰.

Vis dar neaišku, kokios būtų ombudsmeno tyrimo įgaliojimų ribos. Tiek Komisijos sprendimo projektas, tiek Valstybės departamento III priedas šiuo klausimu nėra aiškūs. Darbo grupės supratimu, ombudsmenas turėtų gauti pakankamai informacijos, kad galėtų tvirtinti, ar

⁷⁷ *Kadi II* 100 sk.

⁷⁸ *Kadi II* 119 sk.

⁷⁹ *Kadi II* 125 sk.

⁸⁰ *Kadi II* 122 sk.; nors atitinkama valdžios įstaiga neprivalo pateikti visos informacijos ir įrodymų, pagrindžiančių priemonės taikymo priežastis.

saugumo tarnybos tvarko duomenis pagal įstatymų nuostatas, o jeigu ne, jis privalo užtikrinti, kad netinkama situacija būtų ištaisyta. Tačiau nei Valstybės departamento rašte, nei Komisijos sprendimo projekte nenurodyta, ar ombudsmenas turėtų turėti tiesioginę prieigą prie saugomų duomenų apie asmenį ir gali atlikti savo tyrimą arba ar jis gali vadovautis tik kitų JAV valdžios tarnautojų ataskaitomis.

3.5.3.8 Įgaliojimai imtis taisomųjų veiksmų

Atsižvelgiant į memorandumą, lieka neaišku, kaip ombudsmenas gali nurodyti ištaisyti neatitikimus. Kartu su aiškumo dėl tyrimo įgaliojimų trūkumu lieka neaišku, kiek ombudsmenas kaip toks gali efektyviai nurodyti pašalinti neatitikimą ir koks būtų rezultatas. Ar tai gali reikšti, kad duomenys, kurie buvo gauti netinkamu būdu (t. y. neteisėtai), negali būti naudojami jokiose procedūrose ir turėtų būti ištrinti?

Be to, darbo grupė manė, kad „privatumo skyde“ nenumatyta ombudsmeno galimybė apskusti „sprendimą“ ar jį peržiūrėti.

Galiausiai, kai ombudsmenas susisieks su skundo teikėju išnagrinėjęs skundą, jis negali atskleisti, ar žvalgybos bendruomenė neteisėtai elgėsi. Pateiktas atsakymas visada bus tas pats ir jis bus neaiškus. *Kadi II* byloje ESTT nusprendė, kad kompetentinga įstaiga (kaip priežiūros įstaiga) privalo nurodyti priežastis, kurios apima visas aplinkybes, nors pagal ESTT 296 straipsnį nereikalaujamas išsamus atsakymas⁸¹.

3.5.4 Išvados

Veiksmingos asmenims prieinamos teisių gynybos priemonės ir toliau kelia susirūpinimą DG29. Visų pirma, sprendimo dėl tinkamumo projekte nepateikiamas aiškus atsakymas į klausimą, kokiose situacijose ir kokiomis sąlygomis asmenys gali iškelti bylą, siekdami, kad būtų nustatytos jų teisės.

DG29 pripažįsta ir palankiai vertina alternatyvaus žalos atlyginimo mechanizmo įvedimą ombudsmeno forma, nes tokiu būdu unikalčiai plėtojami santykiai tarp ES ir trečiosios šalies. Be būtinybės paaiškinti terminą „ES asmenys“, kaip nurodyta pirmiau, šiuo mechanizmu sukuriamas papildomas būdas siekti žalos atlyginimo iš JAV administracijos, siekiant, kad būtų užtikrinta, jog bet kokie asmeniniai pareiškėjo duomenys tvarkomi pagal JAV įstatymus.

Tuo pat metu, kai ombudsmeno mechanizmas vertinamas pagal nepriklausomo teismo normas, remiantis Chartijos 47 straipsniu, ir pagal reikalavimus, kuriuos ESTT ir EŽTT nustatė savo praktikoje, stebėjimo byloje, DG29 pastebi žymius trūkumus. Visų pirma, kyla abejonių dėl to, ar ombudsmenas gali būti laikomas (oficialiai ir visiškai) nepriklausomu, ypač dėl to, kad jis gali santykinai lengvai atleisti politinius patikėtinius. Antra, išlieka abejonių dėl ombudsmeno įgaliojimų nuolat efektyviai vykdyti kontrolę. Remiantis III priede pateikta informacija, DG29 negali daryti išvados, kad ombudsmenas visada turės tiesioginę prieigą prie visos informacijos, bylų ir IT sistemų, būtinų, norint atlikti įvertinimą, ar kad jis

⁸¹ *Kadi II* 116 sk.

iš tikrųjų atsakingas žvalgybos agentūras gali priversti nutraukti netinkamą duomenų tvarkymą, jeigu nesutariama dėl klausimo, ar duomenų tvarkymas atitinka įstatymus ar ne. Gali būti, kad tolesnis ombudsmeno pareigų ir įgaliojimų aiškinimas gali pašalinti DG29 abejones.

3.6 Baigiamosios pastabos dėl JAV nacionalinio saugumo įstaigoms taikomų apsaugos priemonių ir apribojimų

Visų pirma, DG29 palankiai vertina Komisijos ir JAV įstaigų pastangas, kurios buvo įdėtos, siekiant didinti skaidrumą, atsižvelgiant į poveikį, kurį JAV stebėjimo programos gali daryti duomenims, kurie perduodami pagal „privatumo skydą“ – ar naudojantis bet koku kitu perdavimo įrankiu. 2013 m. birželio mėn. Snowdenui atskleidus informaciją, buvo imtasi svarbių žingsnių. Nepaisant to, DG29 pažymi, kad vis dar lieka abejonių. Kraštutiniu atveju pagal „privatumo skydą“ būtini papildomi teisių ir įsipareigojimų paaiškinimai.

Pagrindiniai du DG29 susirūpinimą keliantys klausimai yra tai, kad masinis ir plataus masto rinkimas nėra visiškai uždraustas JAV įstaigų ir kad nebuvo tiksliau nustatyti ombudsmeno įgaliojimai ir pareigos. Be to, nacionalinės DAI turėtų būti kompetentingos pradėti procedūras prieš ombudsmeną asmens vardu vietoj žvalgybos agentūrų priežiūros įstaigų. Be to, nors DG29 neabejotinai pripažįsta bandymus išspręsti DAI iškeltus susirūpinimą keliančius klausimus, tolesnės apsaugos priemonės būtų vertinamos labai palankiai, siekiant užtikrinti, kad bet koks JAV stebėjimo programų sąlygotas kišimasis demokratinėje visuomenėje yra būtinas.

4. „PRIVATUMO SKYDO“ TEISĖSAUGOS GARANTIJŲ ĮVERTINIMAS

4.1 Įvadas

Kalbant apie viešąją prieigą prie asmens duomenų teisėsaugos tikslais, DG29 pažymi, kad „privatumo skydo“ II priedo privatumo principuose yra nukrypimas, kuris yra identiškas „saugaus uosto“ privatumo principų nukrypimui. Bendras nukrypimo pobūdis išliko toks pats, o tai reiškia, kad nauji „privatumo skydo“ principai sudaro sąlygas kišimuisi į asmenų, kurių asmens duomenys perduodami iš ES į JAV, pagrindines teises „nacionalinio saugumo ir viešųjų interesų ar Jungtinių Amerikos Valstijų vietos įstatymų pagrindu“⁸².

Tačiau vienas iš pagrindinių teismo kritikos „saugaus uosto“ sprendimui aspektų buvo tas, kad „nepateiktos jokios išvados dėl valstybės priimtų taisyklių, skirtų riboti kišimąsi į asmenų, kurių duomenys perduodami iš Europos Sąjungos į Jungtines Amerikos Valstijas, pagrindines teises, kurios galiotų Jungtinėse Amerikos Valstijose.“

Todėl DG29 palankiai vertina JAV administracijos pastangas pateikti daugiau informacijos apie teisės aktus, reglamentuojančius kėsinimąsi į asmens duomenis, perduotus pagal „privatumo skydą“ teisėsaugos tikslais, įskaitant taikomus apribojimus ir apsaugos priemones. Be to, DG29 pabrėžia, kad visuomenės prieigos suteikimą svarsto, atsižvelgdama į faktą, kad

⁸² Schrems, 87 sk.

bet koks kišimasis į pagrindines teises į privatų gyvenimą ir duomenų apsaugą demokratinėje visuomenėje turi būti pateisintas. Todėl DG29 išanalizavo „privatumo skydo“ suteiktas teisėsaugos garantijas, naudojantis sistema, kaip nurodyta šios nuomonės 1.2 skyriuje.

4.2 Esminių Europos garantijų taikymas teisėsaugos institucijų prieigai prie korporacijų turimų duomenų

4.2.1. Teisėsaugos institucijų prieiga prie asmens duomenų turi atitikti įstatymus ir turi būti paremta aiškiomis, tiksliais ir prieinamomis taisyklėmis

„Privatumo skydo“ VII priede pateiktas raštas iš JAV teisingumo departamento, kuriame pateikta „trumpa pirminių tyrimo įrankių, naudojamų siekiant gauti komercinių duomenų, apžvalga ir kita informacija apie įrašus iš Jungtinių Amerikos Valstijų korporacijų baudžiamosios teisės vykdymo ar viešųjų interesų (civiliniais ir reguliavimo) tikslais, įskaitant nustatytus prieigos apribojimus“.

Visos VII priede minimos procedūros kyla tiesiogiai iš JAV Konstitucijos (Ketvirtosios pataisos), bendrųjų ar proceso teisės aktų arba iš Teisingumo departamento direktyvų ir taisyklių. VII skyriuje nepateikiamos nuorodos į visus teisės aktus, kuriuose numatytos šios procedūros, tačiau atkreipiamas dėmesys į trumpą pačių procedūrų aprašymą. VII priede taip pat minima, kad „yra kitų teisinių pagrindų bendrovėms užginčyti duomenų prašymus iš administracinių agentūrų, atsižvelgiant į konkrečią pramonės sritį ir turimų duomenų tipą“, pateikiant kelis pavyzdžius, pvz., Bankų slaptumo aktas, Sąžiningo kreditinių ataskaitų sudarymo aktas, Teisės į finansinį privatumą aktas.

DG29 pažymi, kad įstatymų, procedūrų ir taisyklių sistema yra fragmentiška ir kad pateiktiems prieigos prašymams taikomos teisės nuostatos priklausys nuo ieškomų duomenų pobūdžio, bendrovės tipo, teisinių procedūrų (baudžiamosios, administracinės, susiję su viešaisiais interesais) ir prieigos prašančio subjekto pobūdžio.

Kadangi visos teisėsaugos institucijų prieigos prie pagal „privatumo skydą“ perduotų duomenų ribojimo taisyklės pagrįstos Konstitucija, bendrosios teisės nuostatomis ir skaidria Teisingumo departamento politika, DG29 atsižvelgia į šių taisyklių prieinamumo prielaidą. Tačiau taisyklių aiškumas ir tikslumas gali būti įvertintas tik kiekvieno procedūros tipo ir prieigos prašymo atveju. Todėl DG29 apgailestaudama pažymi, kad remiantis „privatumo skydo“ VII priede pateiktais duomenimis ir sprendimo projekte pateiktomis išvadomis, šiuo metu tokio įvertinimo neįmanoma atlikti.

4.2.2 Turi būti įrodytas būtinumas ir proporcingumas, atsižvelgiant į siekiamus teisėtus tikslus

DG29 pažymi, kad prieigos prie duomenų teisėsaugos tikslais prašymas gali prisidėti prie teisėtų tikslų siekimo. Pavyzdžiui, remiantis EŽTK 8 straipsnio 2 dalimi, galimas viešųjų įstaigų kišimasis į teisę į privataus gyvenimo apsaugą „visuomeninio saugumo labui, (...)“

siekiant užkirsti kelią tvarkos pažeidimams ar nusikaltimui (...).“ Tačiau toks kišimasis yra priimtinas, tik kai tai yra būtina ir proporcinga⁸³.

Remiantis nusistovėjusia ESTT praktika, atsižvelgiant į proporcingumo principą, būtina, kad teisinės priemonės, kuriomis numatomas kišimasis į teisę į privatų gyvenimą ir asmens duomenų apsaugą, „būtų proporcingos kaip ir siekiant teisėtų tikslų, remiantis *aptariamais teisės aktais*, ir neviršytų ribų, kurios yra tinkamos ir reikalingos, norint siekti tų tikslų“⁸⁴ (pabrėžta mūsų). Todėl reikalingumas ir proporcingumas visada įvertinamas, atsižvelgiant į konkrečią įstatymuose numatytą priemonę.

VII priede JAV valdžios įstaigos nurodo, kad federaliniai prokurorai ir federaliniai tyrimo agentai gali gauti prieigą prie dokumentų ir kitos įrašų informacijos iš organizacijų, vykdydami „kelių tipų privalomas teises procedūras, įskaitant didžiosios žiuri šaukimus, administracinius potvarkius ir kratos orderius“ ir gali įgyti kitų ryšių, „remdamiesi pasiklausomais telefoniniais pokalbiais ir renkamais numeriais registratorių srityje“⁸⁵. Be to, civilines ir reguliavimo pareigas turinčios agentūros gali priimti korporacijoms skirtus šaukimus į teismą „dėl įmonių įrašų, elektroniniu būdu saugomos informacijos ar kitų materialių daiktų“⁸⁶. Be to, VII priede nurodyta, kad šios teisinės procedūros bendrai naudojamos, norint gauti informaciją iš JAV korporacijų, nepaisant to, ar jos yra sertifikuotos pagal „privatumo skydą“ ir „neatsižvelgiant į duomenų subjekto tautybę“. Kitaip tariant, atrodo, kad šios apsaugos objektai yra organizacijos, o ne patys asmenys.

Be to, remiantis VII priedu, sprendimo projekte – kuris yra pagrįstas „privatumo skydo“ principais – pateiktos Komisijos išvados dėl kišimosi į asmenų, kurių asmeniniai duomenys perduodami iš ES į JAV pagal „privatumo skydą“, pagrindines teises ribojimo taisyklės JAV.

Tiksliau, sprendimo projekte pateiktose išvadose minimi galiojantys apribojimai ir apsaugos priemonės pagal JAV Konstitucijos Ketvirtąją pataisą, remiantis kuria teisėsaugos institucijų vykdomoms paieškomis ir areštams iš esmės būtinas teismo išduotas orderis ir pagrįstos priežasties įrodymas⁸⁷. Taip pat minima, kad išimtiniais atvejais, kai reikalavimas dėl orderio netaikomas, teisėsaugos institucijoms taikomas pagrįstumo testas⁸⁸.

Nepaisant to, remiantis pateikta informacija, neaišku, kaip apsaugos priemonės taikomos ne JAV asmenims. Faktiškai sprendimo projekto konstatuojamoje dalyje pripažįstama, kad „apsauga pagal Ketvirtąją pataisą netaikoma ne JAV asmenims, kurie nėra Jungtinių Amerikos Valstijų gyventojai“⁸⁹. Be to, tuose pačiuose sprendimo projekto punktuose tvirtinama, kad ne JAV asmenys „gauna netiesioginę naudą per apsaugą JAV bendrovėms, kurios disponuoja asmens duomenimis ir kurios gauna teisėsaugos užklausas“. Tačiau DG29

⁸³ Žr. Esminių Europos garantijų darbo dokumentą, 7–9 p. Bendras reikalingumo ir proporcingumo įvertinimas pateiktas DG29 „Nuomonė 01/2014 dėl reikalingumo ir proporcingumo bei duomenų apsaugos principų taikymo teisėsaugos sektoriuje“, 2014 m. vasario 27 d.

⁸⁴ *Digital Rights Ireland*, 46 sk. ir cituota teismo praktika.

⁸⁵ VII priedas, 2 p.

⁸⁶ VII priedas, 4 p.

⁸⁷ Sprendimo dėl tinkamumo projektas, 107 sk.

⁸⁸ „Privatumo skydas“, 107 sk.

⁸⁹ Sprendimo dėl tinkamumo projektas, 108 sk.

apgailestaudama pažymi, kad šioje išvadoje nenurodomas teisinis šaltinis teisės aktuose ar teismo praktikoje.

Apibendrinant, DG29 pažymi, kad tyrimo įrankių sistema, naudojama gauti komercinius duomenis ir kitą įrašų informaciją iš Jungtinių Amerikos Valstijų korporacijų baudžiamosios teisėsaugos ar viešųjų interesų tikslais – įskaitant prieigos apribojimus ir apsaugos priemones – yra sudėtinga priemonių sistema. Remiantis prieinama informacija, šiuo momentu ši sistema negali būti bendrai vertinama. Norint iš tikrųjų įvertinti teisėsaugos tyrimų priemonių reikalingumą ir proporcingumą pagrindinių teisių į privatų gyvenimą ir duomenų apsaugą atžvilgiu reikalingas specialus vertinimas konkrečiais atvejais.

4.2.3 Turėtų būti sukurtas nepriklausomas priežiūros mechanizmas

DG29 pabrėžia faktą, kad daugumos VII priede aprašytų procedūrų atveju numatomas teismo sprendimas, prieš valdžios įstaigoms gaunant prieigą prie duomenų (pvz., teismo nutartys dėl renkamų numerių registratorių ir spąstų ir sekimo prietaisų, teismo orderiai dėl stebėjimo pagal Federalinį slapto pokalbių klausymosi įstatymą, kratos orderiai – 41 taisyklė). Tačiau atrodo, kad ne visų jų atveju reikalingas teismo kišimasis *a priori*. Pavyzdžiui, pilietines ir reguliavimo pareigas turinčios institucijos „gali priimti šaukimus į teismą“⁹⁰. Šiais atvejais yra šaukimo pagrįstumo teisminės *ex post* kontrolės galimybė, kadangi „administracinio potvarkio gavėjas gali ginčyti šaukimo įgyvendinimą teisme“⁹¹.

Remdamasi turima informacija, DG29 pažymi, kad atsižvelgiant į teisėsaugos institucijų prieigą prie JAV bendrovių turimų duomenų, gana stambus nepriklausomas priežiūros mechanizmas atrodo tinkamiausias.

4.2.4 Asmenims turi būti užtikrintos veiksmingos teisių gynimo priemonės

Kaip minėta anksčiau, „apsauga pagal Ketvirtąją pataisą netaikoma ne JAV asmenims, kurie nėra Jungtinių Amerikos Valstijų gyventojai“⁹². Tai reiškia, kad ne JAV asmuo negalėtų užginčyti orderių ar teismo šaukimų teisme, pasitelkdamas Ketvirtą pataisą. Sprendimo dėl tinkamumo projekte nurodyta, kad ne JAV asmenys gauna netiesioginę naudą per apsaugą JAV bendrovėms, kurios disponuoja asmens duomenimis ir kurios gauna teisėsaugos užklausas. Tačiau DG29 pažymi, kad netgi jeigu ši apsauga būtų veiksminga, tai nereiškia, kad asmenims prieinamos veiksmingos priemonės, kadangi atrodo, jog teisės į veiksmingas priemones subjektas šiame scenarijuje yra bendrovė, kuri gauna prieigos prašymą, o ne asmuo, dėl kurio duomenų ginčijamasi.

VII priede nepateikiama išsamesnė informacija apie galimas teisės aktuose numatytas priemones, kurios yra prieinamos ne JAV asmenims, kai valdžios įstaigos ar bendrovės neteisėtai teikia ar gauna prieigą prie duomenų turinio.

⁹⁰ VII priedas, 4 p.

⁹¹ VII priedas, 4 p.

⁹² Sprendimo dėl tinkamumo projektas, 108 punktas.

DG29 palankiai vertina faktą, kad neseniai priimtame Teisminio teisių gynimo priemonių akte⁹³ numatomos teisminės teisių gynybės priemonės ne JAV asmenims. Tačiau šios teisės apsiriboja aiškiai apibrėžtomis ieškinio priežastimis: teisė į duomenų koregavimą ir prieiga prie jų ir išlaidos advokatui, kai „paskirtoji Federalinė agentūra ar padalinys“ neleidžia keisti duomenų arba nesuteikia prieigos prie tokių duomenų ir teisės pasinaudoti civilinėmis teisių gynimo priemonėmis, kai duomenys atskleidžiami „tyčia arba sąmoningai“.

Be to, JAV teismų praktika, minima sprendimo projekto konstatuojamosios dalies išnašose, tiksliau *City of Ontario / Quon*⁹⁴, *Maryland / King*⁹⁵ ir *Samson / California*⁹⁶ bylose, nėra tinkama, siekiant įvertinti, ar ne JAV asmenys gali pateikti reikalavimą teismui, siekdami užginčyti privatumo pažeidimo teisėtumą⁹⁷. Visose bylose buvo nagrinėjama JAV asmenų teisė į privatą gyvenimą ir jose pateikiami JAV aukščiausiojo teismo sprendimai, kurie faktiškai riboja Ketvirtosios pataisos taikymą.

Apibendrinant, DG29 pripažįsta ir palankiai vertina Teisminių teisių gynimo priemonių akto priėmimą, tačiau išlieka abejonių, ar pavieniams duomenų subjektams iš tikrųjų yra prieinamų efektyvių teisių gynimo priemonių.

4.3 Baigiamosios pastabos

Todėl DG29 palankiai vertina ir pripažįsta JAV administracijos pastangas pateikti daugiau informacijos apie teisės aktus, reglamentuojančius kėsiniimąsi į asmens duomenis, perduotus pagal ES ir JAV „privatumo skydą“ teisėsaugos tikslais, įskaitant taikomus apribojimus ir apsaugos priemones.

DG29 pažymi, kad teisėsaugos institucijų tyrimo priemonių sistema, įskaitant galiojančius apribojimus ir apsaugos priemones, yra tiek plati, tiek sudėtinga ir kad „privatumo skyde“ pateikta informacija yra glaudi. Todėl remdamasi ribota informacija (t. y. pateikta „privatumo skydo“ VII priede ir sprendimo projekto duomenimis), DG29 apgailestauja, kad negali pateikti išsamaus galiojančių taisyklių prieinamumo, numatomumo ir reikalingumo įvertinimo. Nepaisant kitų DG29 duomenų apie „privatumo skydą“ šioje ataskaitoje, toks įvertinimas gali būti „privatumo skydo“ metinės peržiūros dalis.

Atsižvelgdama į teisėsaugos institucijų prieigą, DG29 pažymi, kad gana stambus nepriklausomos priežiūros mechanizmas yra tinkamas. Be to, DG29 palankiai vertina Akto dėl teisminės teisių gynybės priėmimą, pagal kurį teisės į teisminę teisių gynybą suteikiamos ne JAV asmenims, tačiau DG29 taip pat pažymi, kad šios teisės yra ribotos. Be informacijos,

⁹³ 2015 m. Teisminių teisių gynimo priemonių aktas, H.R. 1428.

⁹⁴ *City of Ontario, Cal. / Quon*, 130 S. Ct. 2619, 2630 (2010).

⁹⁵ *Maryland / King*, 133 S. Ct. 1958, 1970 (2013).

⁹⁶ *Samson / California*, 547 U.S. 843, 848 (2006).

⁹⁷ *Ontario / Quon* byloje teismas nusprendė, kad Ontarijo miestas nepažeidė Ketvirtojoje pataisoje numatytų darbuotojų teisių, kadangi miesto prieiga prie darbuotojo privačių pranešimų turinio buvo pagrįsta, nes ji buvo motyvuojama teisėtų su darbu susijusių tikslų ir mastai nebuvo per dideli. *Samson / California* byloje teismas nusprendė, kad „remiantis Ketvirtąja pataisa, policijos pareigūnui nedraudžiama vykdyti lygtinai atleisto nuo laisvės atėmimo bausmės asmens paiešką“. *Maryland / King* byloje teismas nusprendė, kad kai pareigūnai vykdo areštą dėl galimos priežasties, siekdami sulaikyti įtariamąjį už rimtą pažeidimą ir atvesdinti jį į poskyrį areštui, burnos tepinėlio paėmimas ir analizavimas, siekiant nustatyti DNR, kaip ir pirštų atspaudai ir nuotraukos, yra teisėtos procedūros policijos poskyryje, kurios yra pagrįstos Ketvirtąja pataisa.

kad ne JAV asmuo negalėtų užginčyti orderių ar teismo šaukimų teisme, remdamasis Ketvirtąja pataisa, išlieka abejonių, ar teisėsaugos srityje konkretiems duomenų subjektams prieinamos veiksmingos teisių gynybos priemonės.

5. IŠVADOS IR REKOMENDACIJOS

Visų pirma, DG29 palankiai vertina faktą, kad per penkis mėnesius nuo „saugaus uosto“ atšaukimo buvo pristatytas naujas sprendimo dėl tinkamumo projektas, kuriame pateikta daug patobulinimų, lyginant su ankstesne priemone. Ji ypač palankiai vertina didesnę skaidrumą, kuris užtikrintas, PD internetinėje svetainėje pateikus du „privatumo skydo“ sąrašus: viename sąrašė pateikiami prie „privatumo skydo“ prisijungusių organizacijų įrašai, o kitame sąrašė pateikiami įrašai apie tas organizacijas, kurios prisijungė prie „privatumo skydo“ anksčiau, tačiau nebėra prisijungę. Taip pat palankiai vertinamas didesnis viešosios prieigos prie pagal „privatumo skydą“ perduotų duomenų skaidrumas nacionalinio saugumo ar teisėsaugos tikslais. Galiausiai, DG29 buvo labai malonu sužinoti, kad visos duomenų perdavimo operacijos JAV bus vienodai apsaugotos: nėra specialių teisinių nuostatų, pagal kurias pirmenybė būtų teikiama vienam ar kitam įrankiui.

5.1 Trys nerimą keliantys klausimai

Tačiau išlieka trys nerimą keliantys klausimai, kuriuos DG29 nuomone reikės išspręsti.

Pirmasis klausimas yra tas, kad atsižvelgiant į sprendimo dėl tinkamumo projekte naudojamą kalbą, organizacijos neįpareigojamos ištrinti duomenis, jeigu jie nebereikalingi. Tai yra esminis ES duomenų apsaugos įstatymo elementas, siekiant užtikrinti, kad duomenys nebus saugomi ilgiau nei reikia, norint pasiekti tikslą, kuriuo jie buvo surinkti. Antra, DG29 mano, kad pagal VI priedą JAV administracija nedraudžia tęstinio masinio ir plataus masto duomenų rinkimo. DG29 nuosekliai laikosi nuomonės, kad toks duomenų rinkimas yra nepateisinamas kišimasis į pagrindines asmenų teises. Trečias susirūpinimą keliantis klausimas yra ombudsmeno mechanizmo įvedimas. Netgi DG29 palankiai vertinant šį beprecedentį žingsnį, asmenims sukuriant papildomą teisių gynimo ir priežiūros mechanizmą, išlieka abejonių, ar ombudsmenas turi pakankamai įgaliojimų efektyviai veikti. Siekiant parodyti, kad ombudsmeno funkcijos yra iš tikrųjų nepriklausomos ir užtikrina veiksmingas teisių gynimo priemones netinkamai tvarkant duomenis, reikėtų paaiškinti bent ombudsmeno įgaliojimus ir pareigas.

5.2 Rekomenduojami paaiškinimai

Be pirmiau minėtų klausimų, DG29 savo nuomonėje nurodė įvairius klausimus, kurių atveju reikalingi išsamesni sprendimo dėl tinkamumo paaiškinimai. Svarbiausia, tai galioja poreikiui užtikrinti, kad „privatumo skyde“ naudojamos pagrindinės duomenų apsaugos sąvokos apibrėžtos ir taikomos nuosekliai. Šiuo metu taip nėra. Būtų gerai, jeigu „privatumo skydo“ DUK skyriuje būtų pateiktas terminų žodynas, kuriame būtų pateiktos apibrėžtys, suderintos tarp ES ir JAV. DG29 taip pat pateikia išvadą, kad tolesnis ES asmens duomenų perdavimas yra nepakankamai reglamentuotas, ypač jų apimties, tikslo ribojimo ir perdavimo atstovams

taikomų garantijų atžvilgiu. Teisėsaugos institucijų prieiga prie „privatumo skydo“ duomenų, ypač dėl teisės aktų numatomumo, kelia susirūpinimą dėl plačios ir sudėtingos JAV teisėsaugos sistemos federaliniu ir valstybiniu lygiu bei dėl to, kad sprendime dėl tinkamumo pateikta ribota informacija .

„Privatumo skydas“ yra pirmasis sprendimas dėl tinkamumo, kuris buvo sudarytas, iš esmės suderinus BDAR tekstus. Vis dėl to, daugelis asmenims siūlomų patobulinimų duomenų apsaugos lygiu neatsispindi „privatumo skyde“. Todėl DG29 rekomenduoja peržiūrėti šį sprendimą dėl tinkamumo ir sprendimus dėl tinkamumo kitoms trečiosioms šalims netrukus po BDAR įsigaliojimo.

Čia apžvelgta galutinė DG29 rekomendacija taikoma bendrai peržiūrai. DG29 palankiai vertina faktą, kad sprendimas dėl „privatumo skydo“ tinkamumo iš tikrųjų bus peržvelgiamas kasmet, dalyvaujant DAI ir kitoms susijusioms šalims. Ji palankiai vertintų susitarimą dėl bendrų peržiūrų elementų, įskaitant susitarimus dėl visų šalių peržiūros ataskaitos sudarymo ir pateikimo, gerokai prieš pirmąją peržiūrą.